

Public Document Pack
SOUTHEND-ON-SEA BOROUGH COUNCIL

Audit Committee

Date: Wednesday, 23rd October, 2019

Time: 6.30 pm

Place: Committee Room 1 - Civic Suite

Contact: Colin Gamble (Head of Democratic Services)

Email: committeesection@southend.gov.uk

AGENDA

- 1 Apologies for Absence**
- 2 Declarations of Interest**
- 3 Minutes of the Meeting held on Wednesday, 24th July, 2019**
- 4 Deloitte: Annual Audit Letter, Audit for the year ended 31 March 2019**
Report of the Executive Director (Finance and Resources)
- 5 Control Environment Assurance**
Report of the Executive Director (Finance and Resources)
- 6 A Simple and Effective Governance Framework**
Report of the Executive Director (Legal & Democratic Services)
- 7 Internal Audit Service Quarterly Performance Report**
Report of the Executive Director (Finance and Resources)
- 8 Information Item**
CIPFA Better Governance Forum
 - Audit Committee Update, Helping Audit Committees to Be Effective
- 9 Exclusion of the Public**

To agree that, under Section 100(A)(4) of the Local Government Act 1972, the public be excluded from the meeting for the item of business set out below on the grounds that it will involve the likely disclosure of exempt information as defined in Part 1 of Schedule 12A to the Act, and that the public interest in maintaining the exemption outweighs the public interest in disclosing the information.

Members:

Cllr P Collins (Chair), Cllr L Burton (Vice-Chair), Cllr B Ayling, Cllr T Cox, Cllr M Davidson, Cllr N Folkard, Cllr S Habermel, Cllr M Kelly, Cllr I Shead and K Pandya

SOUTHEND-ON-SEA BOROUGH COUNCIL

Meeting of Audit Committee

Date: Wednesday, 24th July, 2019
Place: Committee Room 1 - Civic Suite

3

Present: Councillor P Collins (Chair)
Councillors L Burton (Vice-Chair), A Bright*, M Davidson, N Folkard,
S Habermel, M Kelly, I Shead and K Pandya
*Substitute in accordance with Council Procedure Rule 31.

In Attendance: J Chesterton, A Barnes, J Ruffle, I Ambrose, C Fozzard, S Putt,
F Abbott, E Allen, C Wisdom (Deloitte) and A Kleiman (Deloitte)

Start/End Time: 6.30 pm - 8.15 pm

252 Apologies for Absence

Apologies for absence were received from Councillor T Cox (substitute Cllr A Bright) and Councillor B Ayling (no substitute).

253 Declarations of Interest

The following declaration of interest was made at this meeting:

(a) Councillor Davidson – agenda item Agenda item 9 (Adoption of the Annual Governance Statement 2018/19 and Statement of Accounts) – Non-pecuniary interest: Non-Executive Director of South Essex Homes.

254 Minutes of the Meeting held on 27th March 2019

Resolved:

That the Minutes of the Meeting held on Wednesday, 27th March, 2019 be confirmed as a correct record and signed.

255 Teachers Pension Return 2017/18 - Progress report

The Committee considered a report of the Strategic Director (Transformation) which updated the Committee on the reasons and actions taken to address questions raised by Members of the Committee at the meeting held in March 2019, with regard to teachers' pensions reconciliations (Minute 798 refers).

Resolved:

To note the comments and assurances provided by officers that processes are in place to mitigate concerns going forward with regard to the Teachers Pensions Return external audit certification arrangements.

256 Internal Audit Service, Quarterly Performance Report 2018/19

The Committee considered a report of the Strategic Director (Finance & Resources) which updated the Committee on progress made in delivering the Internal Audit Strategy for 2018/19.

The Committee asked a number of questions, which were responded to by officers.

With reference to Appendix 1 and the decisions not to progress the audit of the Virtual School, deferred due to external experts undertaking the independent peer review, the Head of Internal Audit confirmed that, to help assurance, he would bring the peer review report to the next meeting of the Committee.

With reference to Appendix 2b, Direct Payment Support Services Contract Management, the Committee asked that the actions taken with regard to contract monitoring be reported to the next meeting of the Committee by the Interim Director Adult Social Care.

With reference to Appendix 2c, South East Active Travel Programme governance arrangements, the Head of Internal Audit said that he would share the results of the full audit, when available and would provide feedback to the Committee at the next meeting.

With regard to Appendix 2d, Audits Revisited, Unit 4 Business World System Access Controls, and that the overarching IT security policies still requiring approval by the Council's SIRO, the Strategic Director (Transformation) is to provide a written response to the Committee on the position before the next meeting.

In response to questions to the responses to the stakeholder survey, detailed at Appendix 3, and the use of 'survey monkey', the Head of Internal Audit said that he would review the survey approach (but still in electronic format) to hopefully increase responses.

Resolved:

That the progress made in delivering the 2018/19 Internal Audit Strategy, be noted.

257 Head of Internal Audit Annual Report 2018/19

The Committee considered a report of the Strategic Director (Finance and Resources) providing the following for the 2018/19 financial year:

- the rationale for and an audit opinion on the adequacy and effectiveness of Southend-on-Sea Borough Council's (the Council's) risk management, control and governance processes; and
- a statement on conformance with the UK Public Sector Internal Audit Standards (the Standards) and the results of the Quality Assurance and Improvement Programme.

The Committee asked a number of questions which were responded to by officers.

On behalf of the Committee, the Chair thanked officers for the report and the successful progress on delivering the Annual Audit Plan.

Resolved:

That the Head of Internal Audit's Annual Report for 2018/19, be accepted.

258 Counter Fraud & Investigation Directorate, Annual Report for 2018/19

The Strategic Director (Finance & Resources) advised the Chair that he had been notified earlier that day that no one from the Counter Fraud & Investigation Team was available to attend the meeting to answer questions of the Counter Fraud Strategy and work programme for 2018/19. The Chair and Committee Members expressed their concerns and asked that these be conveyed to the Counter Fraud & Investigation Team.

The Strategic Director (Finance & Resources) advised that, separately to this, the Council is reviewing its counter fraud policy and procedures and that a report will be submitted to Cabinet at its meeting in September and to the Audit Committee in October. He also advised that there are on-going discussions with Thurrock Council about the costs and value for money of the service.

Resolved:

That the item be withdrawn and the annual performance report be considered at the next meeting of the Committee.

259 Deloitte's: Final Report to Those Charged With Governance 2018/19

The Committee considered a report of the External Auditor summarising the results of the work completed to date for the 2018/19 financial year with regard to:

- The opinion on the Statement of Accounts; and
- The conclusion on the adequacy of the Council's arrangements for securing economy, efficiency and effectiveness in the use of resources (the VFM conclusion).

In introducing the report the External Auditor Partner, Craig Wisdom, updated the Committee to say it was rare to find a finance team so well prepared for audit with all evidence readily available. He praised the early engagement and pre-planning that had taken place.

The Committee asked a number of questions which were responded to by the External Auditor and officers.

On behalf of the Committee, the Chair thanked officers for the successful audit and the smooth transition made to the new team of auditors. The plan is for the audit to be formally 'signed off' by the end of the week.

Resolved:

That the report on the audit for the year ended 31st March 2019, be accepted.

260 Adoption of the Annual Governance Statement 2018/19 and Statement of Accounts 2018/19

The Committee considered a report of the Strategic Director (Finance and Resources) which presented:

- the Annual Governance Statement for 2018/19, together with the actions for 2019/20 and an update on progress made with regard to the 2018/19 action plan; and
- the Statement of Accounts for 2018/19, for adoption.

The Committee asked a number of questions which were responded to by the External Auditor and officers. On behalf of the Committee the Chair thanked the Head of Corporate Finance and his team for all their hard work. The Chair also wished Mr Ambrose every success in his new role at the London Borough of Redbridge.

Resolved:

1. That subject to any further views expressed by External Audit, the Annual Governance Statement for 2018/19 be approved and recommended to the Leader of the Council and Chief Executive for authorisation and signature.
2. That the Statement of Accounts 2018/19 be adopted and approved for publication.

261 Counter Fraud & Investigation Directorate, Counter Fraud Plan and Strategy for 2019/20

Resolved:

That in line with Minute 258 the item be withdrawn and the Counter Fraud & Investigation Strategy and work programme for 2019/20 be considered at the next meeting of the Committee.

262 Audit Committee Self-Assessment

The Committee considered a report of the Strategic Director (Finance and Resources). This presented the findings of the self-assessment of good practice undertaken at the end of 2018/19, as detailed at Appendix 1 to the report. Appendix 2 to the report set out the proposed actions that could be undertaken to enhance the current arrangements of the Audit Committee, enabling it to discharge its responsibilities as effectively as possible, meeting best practice expectations.

The Chair highlighted the recommendation that the Audit Committee produce an annual report for 2019/20 which was fully supported as this will outline its work for Full Council. He also highlighted that there will be a self-evaluation circulated to the Committee members which will enable members to highlight their skills and training needs. This will be sent to substitutes and those who

were substitutes at meetings in the previous municipal year (and who are still Councillors).

The Strategic Director (Finance and Resources) also confirmed the intention to run a training session for Committee members later in the year. This training will be made available to all Councillors.

Resolved:

To note the results of the self-assessment against good practice undertaken at the end of 2018/19 and the actions detailed at Appendix 2 to the report, be approved.

263 Information Item

The Committee received and noted the following information item:

- Audit Committee Update – helping audit committees to be effective – Issue 28: The Audit Committee Role in Supporting Counter Fraud and Anti-corruption (March 2019)

Chair: _____

This page is intentionally left blank

Southend-on-Sea Borough Council

Report of the Executive Director (Finance and
Resources)

to

Audit Committee

on

23 October 2019

Agenda
Item No.

4

Report prepared by: Andrew Barnes, Head of Internal Audit

Deloitte: Annual Audit Letter 2018/19

A Part 1 Public Agenda Item

1. Purpose of Report

- 1.1 To present the External Auditor's Annual Audit Letter for 2018/19 to the Audit Committee.

2. Recommendations

- 2.1 **The Audit Committee approves the Annual Audit Letter for 2018/19.**

3. Background

- 3.1 This Annual Audit Letter summarises the key issues arising from the work Deloitte have carried out during the year as the Council's auditors, and highlights the key findings that should be considered by the Council.
- 3.2 It is intended to be a short document, aimed at the public, to inform them about the results of the audit. It should be posted onto the Council's website and will also be posted on the Public Sector Audit Appointments (PSAA) website.

4. Reasons for Recommendations

- 4.1 **The production and publication of an Annual Audit Letter is a requirement of the National Audit Office's Code of Audit Practice (the Code).**

5. Corporate Implications

- 5.1 Contribution to the Southend 2050 Road Map

Audit work provides assurance and identifies opportunities for improvements that contribute to the delivery of all Southend 2050 outcomes.

- 5.2 Financial Implications

The fee for the audit work is set by Public Sector Audit Appointments Limited and agreed with the Council before the start of the audit. The code audit fee for 2018/19 was £109,968. Issues arising during the course of the audit can impact on the audit fee payable.

5.3 Legal Implications

The Council is required to have an external audit of its activities that complies with the requirements of the Code. By considering this report, the Committee can satisfy itself that this requirement is being discharged.

5.4 People Implications

None

5.5 Property implications

None

5.6 Consultation

The Annual Audit Letter for 2018/19 has been discussed and agreed with the Executive Director (Finance and Resources).

5.7 Equalities and Diversity Implications

None

5.8 Risk Assessment

Periodically considering whether the external auditor is delivering the agreed Annual Audit Plan helps mitigate the risk that the Council does not receive an external audit service that complies with the requirement of the Code.

5.9 Value for Money

PSAA sets the fee formula for determining external audit fees for all external auditors.

5.10 Community Safety Implications

None

5.11 Environmental Impact

None

6. Background Papers

- The Accounts and Audit Regulations 2015
- National Audit Office: Code of Audit Practice

7. Appendices

Appendix 1: Deloitte's Annual Audit Letter 2018/19



Annual Audit Letter on the 2018/19 External Audit Southend-on-Sea Borough Council

October 2019

Deloitte Confidential: Government and Public Services – For Approved External Use Only

Contents

| | Page |
|------------------------------|------|
| 1 Letter to Members | 3 |
| 2 Key Messages | 4 |
| 3 Responsibilities and Scope | 5 |
| 4 Audit of the Accounts | 6 |
| 5 Value for Money | 10 |
| 6 Other Matters | 11 |

1. Letter to Members

The Members
Southend-on-Sea Borough Council
Civic Centre
Victoria Avenue
Southend-on-Sea
SS2 6ER

14 October 2019

Dear Sirs

We have pleasure in setting out this Annual Audit Letter to summarise the key matters arising from the work that we have carried out in respect of the audit for the year ended 31 March 2019.

Although this letter is addressed to the Members of Southend-on-Sea Borough Council ("the Authority"), it is also intended to communicate the significant issues we have identified in an accessible style to key external stakeholders including members of the public. The letter will be published on the Public Sector Audit Appointments Ltd (PSAA) website at www.psaa.co.uk and on the Authority's website.

This letter has been prepared in the context of the Statement of Responsibilities of Auditors and Audited Bodies issued by Public Sector Audit Appointments Ltd. This is available from www.psaa.co.uk.

This letter has been discussed and agreed with the Strategic Director (Finance and Resources). A copy of the letter will be provided to all Members.

This is our first year as the external auditor of the Authority following the transition to the PSAA contract in 2018/19. We would like to take this opportunity to thank management for the assistance and support that enabled this first year of audit to run smoothly.

Yours faithfully,



Craig Wisdom
Audit Partner
for and on behalf of Deloitte LLP
St Albans, United Kingdom

2. Key Messages

Statement of Accounts

Unqualified opinion issued on 30 July 2019

In 2018/19 the Authority was required to prepare its Statement of Accounts in accordance with International Financial Reporting Standards ("IFRS") as defined in the Code of Practice on Local Authority Accounting in the United Kingdom 2018/19 and other relevant legislation.

The Statement of Accounts was prepared and audited in accordance with the agreed timetable.

We issued our audit opinion on the financial statements on 30 July 2019. Our opinion was not qualified.

Materiality for the Authority's accounts was set at £7.4m.

Value for Money ("VfM") conclusion

Unqualified conclusion issued on 30 July 2019

We are required to base our statutory VfM conclusion on the criteria specified by the National Audit Office. This is an evaluation of whether the Authority has in place proper arrangements to ensure properly informed decisions were taken and the Authority deployed resources to achieve planned and sustainable outcomes for taxpayers and local people.

We issued an unqualified VfM conclusion on 30 July 2019.

Audit findings

We did not identify any significant weaknesses in internal control or other findings

International Standards on Auditing (UK) require us to communicate in writing to those charged with governance the significant findings from our audit. For the avoidance of doubt, in respect of the Authority's audit for 2018/19, there were no findings that we brought to the attention of the Audit Committee.

Independence and Objectivity

Independence and objectivity

An analysis of audit fees for the year ended 31 March 2019 is shown in Section 6 of this letter.

In our professional judgement the policies and safeguards in place ensure that we are independent within the meaning of all regulatory and professional requirements and that the objectivity of the audit partner and audit staff is not impaired.

3. Responsibilities and Scope

Responsibilities of the Authority and Auditors

The Authority is responsible for maintaining the control environment and accounting records and preparing the accounting statements in accordance with the Code of Practice on Local Authority Accounting in the United Kingdom 2018/19 based on IFRS and other relevant legislation.

We are appointed as the Authority's independent external auditors by PSAA, the body responsible for appointing auditors to local public bodies in England where they have opted into this programme.

As the Authority's appointed external auditor, we are responsible for planning and carrying out an audit that meets the requirements of the National Audit Office's Code of Audit Practice ("the Code"). Under the Code, we have responsibilities in two main areas:

- auditing the Authority's accounts; and
- evaluating whether the Authority has made proper arrangements for securing economy, efficiency and effectiveness in its use of resources (the value for money ("VFM") conclusion).

The scope of our work

We conducted our audit in accordance with International Standards on Auditing (UK and Ireland) as adopted by the UK Auditing Practices Board ("APB"). The audit opinion on the accounts reflects the financial reporting framework adopted by the Authority, being the Code of Practice on Local Authority Accounting in the United Kingdom 2018/19 based on IFRS and other relevant legislation.

We conducted our work on the 2018/19 VFM conclusion in line with guidance issued by the National Audit Office in November 2017.

4. Audit of the Accounts

| Statement of Accounts | |
|---|--|
| Unqualified opinion issued on 30 July 2019 | <p>We issued an unqualified opinion on the Authority's 2018/19 accounts on 30 July 2019.</p> <p>Before we give our opinion on the accounts, we are required to report to those charged with governance (here the Audit Committee) any significant matters arising from the audit. To address this requirement, a detailed report was issued on 17 July 2019. This was discussed with the members of the Audit Committee on 25 July 2019. This paper is available to view online as part of the Committee pack for that meeting.</p> |
| Materiality | <p>We define materiality as the magnitude of misstatement in the financial statements that makes it probable that the economic decisions of a reasonably knowledgeable person would be changed or influenced. We use materiality both in planning the scope of our audit work and in evaluating the results of our work.</p> <p>Based on our professional judgement, materiality for the Authority's accounts was set at £7.4m which equated to 2% of estimated gross expenditure at the planning stage of the audit. Our materiality for the Group Accounts was set at the slightly higher level of £7.5m. This benchmark was chosen as the Authority is a non-profit organisation and total expenditure is a key measure of financial performance for users of the financial statements.</p> <p>We agreed with the Audit Committee that we would report to the Committee all uncorrected audit differences in excess of £370k, as well as differences below that threshold that, in our view, warranted reporting on qualitative grounds. We would also report to the Audit Committee on any uncorrected disclosure matters identified when assessing the overall presentation of the financial statements. For the avoidance of doubt, no such matters were identified in relation to the audit of the 2018/19 Statement of Accounts.</p> |
| Significant Risks | <p>Our audit work was designed to specifically address the following significant audit risks which are presented in further detail below. Significant audit risks are the areas deemed to be those with the greatest potential of being materially incorrect in the financial statements and are therefore areas of greater focus for the audit team.</p> <ol style="list-style-type: none"> 1. Property valuation: Our conclusion in this risk area is that the net book value of property assets is not materially misstated. The Council's valuation assumptions are generally reasonable and fall within the expected range. There are no other findings to report. <ul style="list-style-type: none"> • Risk identified: <p>The Council is required to hold property assets within Property, Plant and Equipment and Investment Properties at valuation. The valuations are by nature significant estimates which are based on specialist and management assumptions and which can be subject to material changes in value</p> • Deloitte response |

| | |
|--|---|
| | <ul style="list-style-type: none"> ○ We tested the design and implementation of key controls in place around the property valuation, including how the Council assures itself that there are no material impairments or changes in value for the assets not covered by the annual valuation. ○ We obtained an understanding of approach adopted to the valuation, including assessing the valuer's qualifications, objectivity and independence and reviewing the methodology used. ○ We tested a sample of inputs to the valuation. ○ We used our valuation specialists, Deloitte Real Estate, to review and challenge the appropriateness of the assumptions used in the valuation of the Council's property assets including considering the assumptions made of movements between the valuation being performed at earlier stages in the year and the year-end. ○ We tested a sample of revalued assets and reperformed the calculation of the movement to be recorded in the financial statements to check correctly recorded. ○ We considered the impact of uncertainties relating to the UK's exit from the EU upon property valuations in evaluating the property valuations and related disclosures. <p>2. <u>Capital Expenditure:</u> We concluded satisfactorily in this area and there are no findings to report.</p> <ul style="list-style-type: none"> • Risk identified <p>The Council has a substantial capital programme of £233m over the next three years. The capital programme included £50.9m spend in 2018/19. Determining whether or not expenditure should be capitalised can involve judgement as to whether costs should be capitalised. The Council has greater flexibility over the use of revenue resource compared to capital resource. There is also, therefore, a potential incentive for officers to misclassify revenue expenditure as capital.</p> • Deloitte response <ul style="list-style-type: none"> ○ We tested the design and implementation of controls around the capitalisation of costs. ○ We selected a sample of capital items in the year to test whether they have been appropriately capitalised in accordance with the accounting requirements. <p>3. <u>Management override of controls:</u> We concluded satisfactorily in this area. We did not identify any significant bias in the key judgements made by management based on work performed. Furthermore, we have not identified any instances of management override of controls in relation to the specific transactions tested based on work performed. There are no other findings to report</p> <ul style="list-style-type: none"> • Risk identified <p>This risk area includes the potential for management to use their judgement to influence the financial statements as well as the potential to override the Council's controls for specific transactions.</p> |
|--|---|

| | |
|---|---|
| | <ul style="list-style-type: none"> Deloitte response <ul style="list-style-type: none"> We have considered the overall sensitivity of judgements made in preparation of the financial statements, and note that: <ul style="list-style-type: none"> The Council's results throughout the year did project both positive and negative divergences from budgets in operational areas. This was closely monitored and, overall, the contingency budget was not drawn on. Senior management's remuneration is not tied to particular financial results. <p>We have considered these factors and other potential sensitivities in evaluating the judgements made in the preparation of the financial statements.</p> Significant and unusual transactions: We did not identify any significant transactions outside the normal course of business or any transactions where the business rationale was not clear. Journals: We have performed design and implementation testing of the controls in place for journal approval. We have used Spotlight data analytics to risk assess journals and select items for detailed follow up testing. The journal entries were selected using computer-assisted profiling based on areas which we consider to be of increased interest. We have tested the appropriateness of journal entries recorded in the general ledger, and other adjustments made in the preparation of financial reporting. Accounting estimates: We have performed design and implementation testing of the controls over key accounting estimates and judgements. We reviewed accounting estimates for biases that could result in material misstatements. We note that, overall, the areas more subject to estimation in the period were balanced and did not indicate a bias to achieve a particular result. We tested accounting estimates and judgements, focusing on the areas of greatest judgement and value. Our procedures included comparing amounts recorded or inputs to estimates to relevant supporting information from third party sources. |
| Overall opinion | We issued an unqualified opinion on the Authority's 2018/19 accounts on 30 July 2019, in accordance with the deadline set for local government bodies. Our opinion confirms that the accounts present a true and fair view of the financial position of the Authority as at 31 March 2019 and its income and expenditure for the year then ended. |
| Annual Governance Statement and Other Information | |
| No issues were identified in relation to this work | As appointed auditors, we review the Annual Governance Statement ("AGS") and other information presented with the financial statements to check that information is consistent with the financial statements. We do not have any findings to report in relation to this. |

| Powers and Duties | |
|--|--|
| We did not receive any questions about the accounts or make any public interest reports | <p>Under the Local Audit and Accountability Act 2014, auditors have specific powers and duties, including to give electors the opportunity to raise questions about the accounts and to consider and decide upon objections received in relation to the accounts. We did not receive any such questions or objections.</p> <p>We have a duty to consider whether to issue a report in the public interest about something we believe the Authority should consider, or if the public should know about.</p> <p>We have not identified any matters that would require us to issue a public interest report.</p> |
| Whole of Government accounts return | |
| The Authority is below the audit threshold | <p>The Authority prepares a consolidation pack to support the production of Whole of Government Accounts by HM Treasury. We are not required to review this pack as the Authority falls below the threshold where an audit is required. As required by the guidance we have confirmed this with the National Audit Office by the national deadline of 13 September 2019.</p> |
| Audit Certificate | |
| We have issued our certificate | <p>We issued our certificate on 30 July 2019. The certificate confirms that we have concluded the audit for 2018/19 in accordance with the requirements of the Local Audit & Accountability Act 2014 and the Code of Audit Practice.</p> |

5. Value for Money

Background and approach

We are required to issue a value for money ("VfM") conclusion within our report on the financial statements. We are required to base our VfM conclusion on criteria specified by the National Audit Office ("NAO") where we are required to be satisfied that proper arrangements have been made to secure economy, efficiency and effectiveness in the use of resources. Our assessment is based on the following reporting criterion:

"In all significant respects, the audited body had proper arrangements to ensure it took properly informed decisions and deployed resources to achieve planned and sustainable outcomes for taxpayers and local people."

The following sub-criteria are then used to inform and guide our work and inform our overall judgement although there is no requirement to separate these nor to report against each sub-criteria:

- Informed decision making
- Sustainable resource deployment
- Working with partners and other third parties.

We would emphasise that it is the arrangements in place that we are required to assess, and not the actual decisions made by the Authority.

We planned our local programme of work based on our risk assessment, which was informed by a series of risk factors determined by the National Audit Office.

We did not identify any significant risks as part of our risk assessment.

The VFM conclusion

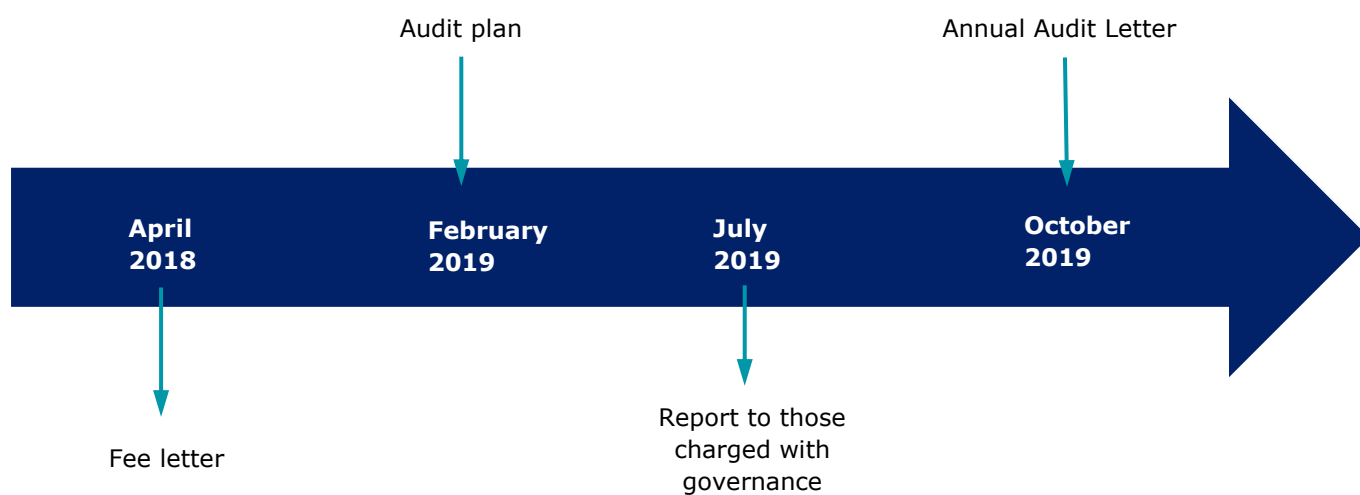
Having performed our work in line with guidance received from the National Audit Office we issued an unqualified value for money conclusion for the 2018/19 financial year.

6. Other Matters

Reports issued

Reports issued during the course of the 2018/19 audit included:

- Audit Fee letter;
- Annual Audit Plan;
- The Report to Those Charged with Governance on the 2018/19 audit of the Authority; and
- This Annual Audit Letter.



Analysis of audit fees

Audit fees charged to date are as follows:

| | 2018/19 £000 |
|---|-----------------|
| Scale fees for the audit of the Authority's annual accounts, VfM conclusion and whole of government accounts return | 110 |

Statement of Responsibilities

The Statement of Responsibilities of Auditors and Audited Bodies issued by PSAA explains the respective responsibilities of auditors and of the audited body and this report is prepared on the basis of, and our audit work is carried out in accordance with, that statement.

The matters raised in this report are only those that came to our attention during our audit and are not necessarily a comprehensive statement of all weaknesses that exist or of all improvements that might be made. You should assess recommendations for improvements for their full implications before they are implemented. In particular, we would emphasise that we are not responsible for the adequacy and appropriateness of the national data and methodology supporting our value for money conclusion as they are derived solely from the National Audit Office.

This report has been prepared for the Members, as a body, and we therefore accept responsibility to you alone for its contents. We accept no duty, responsibility or liability to any other party.

An audit does not provide assurance on the maintenance and integrity of the website, including controls used to achieve this, and in particular on whether any changes may have occurred to the Annual Audit Letter since first published. These matters are the responsibility of the Authority but no control procedures can provide absolute assurance in this area.



This document is confidential and it is not to be copied or made available to any other party. Deloitte LLP does not accept any liability for use of or reliance on the contents of this document by any person save by the intended recipient(s) to the extent agreed in a Deloitte LLP engagement contract.

If this document contains details of an arrangement that could result in a tax or National Insurance saving, no such conditions of confidentiality apply to the details of that arrangement (for example, for the purpose of discussion with tax authorities).

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 1 New Street Square, London, EC4A 3HQ, United Kingdom.

Deloitte LLP is the United Kingdom affiliate of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NSE LLP do not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

© 2019 Deloitte LLP. All rights reserved.

This page is intentionally left blank

Southend-on-Sea Borough Council

Report of Executive Director (Finance and Resources)

To

Audit Committee

On

23 October 2019

Report prepared by: Andrew Barnes (Head of Internal Audit)

Agenda
Item No.

5

Control Environment Assurance

Part 1 (Public Agenda Item) - except for Appendix F which is not for publication by virtue of paragraph 7 of Part 1 to Schedule 12A to the Local Government Act 1972

1. Purpose of Report

To update the Audit Committee on the revisions that have been made to the Control Environment in respect of Risk Management, Counter-Fraud, Bribery & Corruption, Counter Money Laundering, Whistleblowing and the Regulation of Investigatory Powers.

2. Recommendations

- 2.1 That Audit Committee approves the revised Risk Management Policy Statement and Strategy (**Appendix A**, including the action plan included at Appendix 2 of that document).
- 2.2 That Audit Committee approves the revised Counter Fraud, Bribery & Corruption Policy and Strategy (**Appendix B**), the revised Counter Money Laundering Policy & Strategy (**Appendix C**) and the revised Whistleblowing Policy (**Appendix D**).
- 2.3 That Audit Committee approves the revised Policy and Procedures for undertaking Directed Surveillance and the use of Covert Human Intelligence Sources (CHIS) (**Appendix E** – and also the detailed procedures for use of a CHIS as set out in confidential **Appendix F**).
- 2.4 To note that:
 - (a) The Council has not used the surveillance powers available to it under RIPA between 1 April 2018 and the 31st March 2019 and neither has it used any CHIS during this period
 - (b) Thurrock Council has not used any such powers on behalf of Southend-on-Sea Borough Council when undertaking Anti-Fraud work between 1 April 2018 and the 31st March 2019.
- 2.5 To note the staff training undertaken in 2018/19 and proposed for 2019/20 in connection with RIPA - also details of the regulation of CCTV activities as detailed in the report.

3. Risk Management

- 3.1 The Council's risk policy, strategy and toolkit was last formally reviewed in June 2015. As a result of the changes being made to the governance architecture to deliver the Southend 2050 Ambition and Outcomes a review of the Council's approach to risk management has been undertaken by the senior officer Good Governance Group and the Corporate Management Team (CMT).
- 3.2 The Policy Statement and Strategy have, therefore, been reviewed and updated to align with changes to Council policy, structures and resources since 2015. The review found that while the overall approach to corporate risk is sound, some areas required updating and there was a need to update the approach in response to the changes that are being implemented to the culture and governance arrangements of the Council. The main points of note are:
- The changes to reflect the new governance arrangements implemented by the Council to deliver the 2050 Ambition
 - Enhancements to use of risk appetite and tolerance included to reflect a desire for the Council to increasingly focus on where it is prepared to take risks and exploit opportunities to deliver the desired outcomes
 - A simplified scoring system for the risk matrix
 - The roles and responsibilities for groups and individuals have been updated.
- 3.3 The current position in relation to the Council's approach to risk is that:
- The Corporate Risk Register (CRR) is reported to the Council's Corporate Management Team quarterly and Cabinet every 6 months – it is proposed that this continues
 - Risk registers, following the format of the CRR, are included in Service Plans – it is proposed that this is updated to reflect the new governance arrangements
 - Risk registers are included in major council project plans, and the risks monitored regularly, although the format may vary, depending on project requirements – it is proposed that this continues with the format simplified to achieve increased engagement and utilisation
 - High level risks are monitored as part of reports to Corporate Delivery and Capital Boards – it is proposed that this continues, but with reporting to the new governance groups as necessary
 - Risk is a regular item at CMT meetings, and is discussed regularly at Departmental Management Teams – it is proposed that this continues, supported by the risk management resource available.
- 3.4 The Cabinet have reviewed the Policy Statement and Strategy (**Appendix A**), prior to further work to shape, disseminate and implement across the Council, in accordance with Appendix 2 of the Policy Statement and Strategy.

4. Counter-Fraud, Bribery & Corruption, Counter Money Laundering and Whistleblowing

- 4.1 The Counter Fraud, Bribery & Corruption policy and strategy (**Appendix B**) is designed to advise council workers and suppliers on what fraud, bribery and corruption is, how to identify it and report it. This policy sets out what the council will do to make it the most difficult environment for fraud to occur and the responsibility on everyone in the council to find fraud and report it.
- 4.2 Money laundering is a serious crime and recognised as a 'critical enabler' for organised criminal gangs and terrorists to benefit from and use for other criminality. Denying criminals the use of their ill-gotten gains disrupts criminality and can help law enforcement identify offenders. The Counter Money Laundering policy & strategy (**Appendix C**) is designed to advise council workers and suppliers on what money laundering is, how to identify it and report it and sets out the action we will take to mitigate the risk that money could be laundered through our systems.
- 4.3 The Whistleblowing Policy (**Appendix D**) provides arrangements to raise any serious concerns that employees, workers or contractors have about any aspect of service provision or the conduct of Councillors, officers of the Council or others acting on behalf of the Council.
- 4.4 The policies have been updated to reflect changes in legislation, reporting methods and current best practice.
- 4.5 The Council's counter fraud service has been run in partnership with Thurrock Council through the Counter Fraud Investigation Directorate since 2013. However the direction that Thurrock Council want to take the Counter Fraud Investigation Directorate in, and particularly the resources that they want to dedicate into that service to deliver that direction, are no longer consistent with the expectations and requirements of Southend Council and therefore the joint working has been brought to an end. As a result Southend has taken back the staff that were employed by Southend, but shared with Thurrock in their Counter Fraud Investigation Directorate, to re-form Southend Council's own dedicated Counter Fraud team, that continues to deliver the service while the specific arrangements for the working of the counter fraud service are reviewed over the forthcoming period.

5. Directed Covert Surveillance and Regulation of Investigatory Powers Act

- 5.1 If the Council wants to carry out directed covert surveillance then:
 - (a) It must be in connection with the investigation of a criminal offence which attracts a maximum custodial sentence of 6 months or more, or involves the underage sale of alcohol or tobacco;
 - (b) It must not be intrusive surveillance (only the Police can carry out intrusive surveillance inside a house or vehicle);

- (c) Such surveillance must be properly authorised internally. In particular authorising officers must be formally designated and trained – and only authorised and trained officers should carry out surveillance;
- (d) A Justice of the Peace must make an Order approving the grant of authorisation referred to in (c) above; and
- (e) There must be compliance with the Codes of Practice issued by the Home Office, the Investigatory Powers Commissioner's Office (IPCO) (formerly the Office of Surveillance Commissioners OSC) – and the Council's own Policy & Procedures (see 5.3 below).

Covert Human Intelligent Source and Regulation of Investigatory Powers Act

- 5.2 Similar requirements to those set out in 5.1 above apply if the Council wants to use a covert human intelligent source (CHIS). The requirement for the use of CHIS is that it relates to the prevention and detection of crime or disorder; there is no requirement for the offence to have a 6 month sentence.

Council Policy and Procedures for undertaking Directed Covert Surveillance and the use of a CHIS

- 5.3 In order to ensure that the Council acts legally and properly and complies with RIPA, it has put in place "Policy and Procedures for undertaking Directed Covert Surveillance and the use of Covert Human Intelligence Sources (CHIS)".
- 5.4 The Policy & Procedures are regularly updated to ensure they are fit for purpose and incorporate legislative, procedural and staff changes (**Appendix E**). The most significant change is that the detailed procedures for the use of a CHIS are now set out in a separate document (confidential **Appendix F**). The Policy and Procedures also includes a revised section on the use of social media for research and investigations (as this has been the focus of IPCO attention) and clarification of joint agency surveillance to reflect current practice.

Use of surveillance powers available under RIPA in 2018/19

- 5.6 The Council has not used the surveillance powers available to it under RIPA between 1 April 2018 and the 31st March 2019 and neither has it used any CHIS during this period.
- 5.7 Thurrock Council has not used any such powers on behalf of Southend-on-Sea Borough Council when undertaking Anti-Fraud work between 1 April 2018 and the 31st March 2019.

Training

- 5.8 It is important that Council officers who are, or could be, involved with surveillance receive proper training.
- 5.9 Annual training was carried out on the 10 December 2018, attended by 39 members of staff with a focus on awareness of RIPA requirements and also the use of social media for research and investigations.

- 5.10 In 2019/20 a CHIS training session has already been held with 6 members of staff from Regulatory Services and the regular annual training event is planned for early December 2019.

CCTV

- 5.11 The Council's CCTV System helps to provide a safe and secure environment in the Town Centre and other parts of the town covered by the cameras. It therefore contributes to the continuing safety and vitality of those areas, for the benefit of all those living, working and visiting there.
- 5.12 The control room is manned twenty-four hours a day 365 days a year by Security Industry Authority (SIA) trained operators and is fully compliant with the guidelines laid down by the IPCO and the Surveillance Camera Commissioner (SCC).
- 5.13 The inspections by the OSC (now the IPCO) as referred to in 5.14 (below), have always involved a visit to the control room to ensure compliance with the guidelines; although it should be noted that overt CCTV does not require a formal RIPA authority. In 2018 the control room was involved in 8566 incidents that were covered by CCTV which involved 739 arrests being made. This highlights the value of the CCTV System.

Oversight

- 5.14 The IPCO provides independent oversight of the use of investigatory powers by intelligence agencies, police forces and other public authorities. The Council is subject to inspection by the IPCO to ensure compliance with the statutory provisions which govern surveillance. The Council's last inspection was in August 2016 and was carried out by the former OSC: This presented a very positive picture.
- 5.15 It is also important that councillors should review the Council's use of RIPA and its Policies and Procedures on an annual basis; hence the need for this report.

6. Other Options

None

7. Reasons for Recommendations

To comply with the Home Office Codes of Practice and IPCO Guidance on RIPA.

8. Corporate Implications

8.1 Contribution to Southend 2050 Road Map

The Corporate Assurance and Risk Framework underpins the operational effectiveness of the Council's Corporate Governance arrangements and helps the management of key risks associated with achieving the Council's Ambition

and Outcomes. Contributing to and monitoring progress with the Corporate Risk Register reinforces the effectiveness of these arrangements and assists to ensure that Outcomes are delivered.

Work undertaken to reduce fraud and enhance the Council's anti-fraud and corruption culture contributes to the delivery of all Southend 2050 outcomes.

Sound policies and procedures in respect of surveillance contribute to various aspects of the Southend 2050 Road Map, particularly the objective in Safe & Well that people in all parts of the Borough feel safe and secure at all times.

8.2 Financial Implications

The funding of risk management activities across the Council is generally contained within individual budgets.

Proactive fraud and corruption work acts as a deterrent against financial impropriety and might identify financial loss and loss of assets. Any financial implications arising from identifying and managing the fraud risk will be considered through the normal financial management processes. Proactively managing fraud risk can result in reduced costs to the Council by reducing exposure to potential loss and insurance claims.

8.3 Legal Implications

The Accounts and Audit Regulations 2015 Section 3 requires that:

'The relevant authority must ensure that it has a sound system of internal control which:

- facilitates the effective exercise of its functions and the achievement of its aims and objectives*
- ensures that the financial and operational management of the authority is effective*
- includes effective arrangements for the management of risk.'*

The proposed risk management arrangements ensure that the Council is compliant with this requirement.

The Home Office and IPCO provide guidance in respect of RIPA. This report has been prepared to ensure compliance with that guidance.

8.4 People Implications

Failure to manage the corporate risks could have a major impact upon the resources available to the Council and the ability to deliver identified outcome priorities.

Where fraud or corruption is proven the Council will:

- take the appropriate action which could include disciplinary proceedings, civil law and criminal prosecution
- seek to recover losses using criminal and civil law

- seek compensation and costs as appropriate.

8.5 Property Implications

None, but identified as part of the corporate and other risk registers.

8.6 Consultation

Internal only

8.7 Equalities and Diversity Implications

None

8.8 Risk Assessment

The report is aimed to enhance the Council's ability to assess and manage risk in achieving its Ambition and Outcomes.

Failure to operate a strong anti-fraud and corruption culture puts the Council at risk of increased financial loss from fraudulent or other criminal activity. Although risk cannot be eliminated from its activities, implementing these strategies will enable the Council to manage this more effectively.

Having up to date RIPA Policy and Procedures and a staff training programme, ensures any risks associated with surveillance, social media investigations or the use of a CHIS are minimised.

8.9 Value for Money

Effective forecasting and timely management of risk is a key factor in preventing waste, inefficiency and unnecessary or unplanned use of resource.

An effective counter fraud and investigation directorate should save the Council money by reducing the opportunities to perpetrate fraud, detecting it promptly and applying relevant sanctions where it is proven.

8.10 Community Safety Implications

None, but identified as part of the corporate and other risk registers.

8.11 Environmental Impact

None, but identified as part of the corporate and other risk registers.

9. Background Papers

None

10. Appendices

Appendix A - Risk Management Policy Statement and Strategy 2019

Appendix B - Revised Counter Fraud, Bribery & Corruption Policy & Strategy

Appendix C - Revised Counter Money Laundering Policy & Strategy

Appendix D - Revised Whistleblowing Policy

Appendix E - Updated Council Policy and Procedures for undertaking Directed Surveillance and the use of Covert Human Intelligence Sources

Appendix F (Part 2) - Detailed Council Procedures for use of Covert Human Intelligence Sources (CHIS)

RISK MANAGEMENT POLICY STATEMENT & STRATEGY

Approved by:
Corporate Management Team: 7 August 2019
Cabinet: 17 September 2019

Next Planned Review:
2021



Risk Management Policy

The focus for Southend Borough Council is set out within the 2050 ambition and in delivering against the desired outcomes, to fulfil that ambition, decisions are taken regarding allocation of increasingly finite resources. The Council has needed to become more innovative and commercially minded in order to exploit opportunities whilst still operating in an environment where there are high expectations around transparency, integrity and accountability. Delivering value for money remains at the heart of good governance in local authorities.

The Council's Risk Management Framework needs to evolve, along with other elements of the governance framework, to support the achievement of the 2050 outcomes. There are a number of core principles at the heart of the new Council's Risk Management Framework, these include that:

- risk management is a positive value added activity, focused on achievement and successes, not a negative bureaucracy – by changing the perception and raising awareness officers will have increased confidence when managing operational risks
- all staff are responsible for risk management and resources that support the framework are there to 'support and challenge' not 'own and do'
- wider Member involvement in identifying and monitoring the most strategic risks the organisation faces would add value, whilst the roles of the Audit Committee, Scrutiny and Cabinet are critical to robustness of the overall framework
- the Southend 2050 ambition and outcomes need to drive the Council's budget and financial management arrangements, performance management of the outcome delivery plans and risk management framework
- by getting the conversations happening with the right people, at the right time and in the right place, the required thinking can be applied and the processes to capture, document and report risks will be simple and become part of business as usual
- the framework ensures joined up Strategic, Operational, Programme and Project Risk Management whilst recognising the differences between them.

It is important for everyone to recognise that:

**Risk management is not about being 'risk averse' –
it is about being 'risk aware'.**

Risk is ever present and some amount of risk taking is necessary if the Council is to achieve its ambition. In the current climate the council will embark on more risky activities in pursuit of greater outcomes for residents, however the actions to mitigate those risks must bring the risk exposure within the appetite and tolerance approved by members. By being '**risk aware**' the Council is in a better position to mitigate threats and take advantage of opportunities.

The Council will achieve effective Risk Management by:

- implementing this Strategy and a process that is fit for purpose, compliments and strengthens the other governance arrangements within the 2050 programme, including assurance and performance management processes
- ensuring that the management structure is not a barrier to sharing the ownership of risks or the efficiency in the control environment
- equipping managers with the skills and understanding to ensure that robust risk decisions happen across the Council
- ensuring a consistent understanding of the organisation's risk appetite so that effective communication, escalation and cascade, exists across the Council
- acknowledging that risks are increasingly shared across partner organisations, which can increase the complexity of analysis and reporting, and also that assurances regarding the level of risk may need to be sought from third parties as well as internal sources, and that these bodies may need support from the Council to achieve efficient risk management.

We will also annually review the:

- effectiveness of Risk Management activity during the year
- completion of the Risk Management action plan
- approach to ensure it remains in line with good practice.

Every two years we will review and update the formal Policy and Strategy document.

CHIEF EXECUTIVE

LEADER

.....

.....

Risk Management Strategy

Introduction

The Council's Members and Corporate Management Team recognise:

- the importance of effective mechanisms to identify, analyse, manage and monitor risk and for effective channels of communication about risk within the organisation
- their statutory responsibilities for Risk Management particularly in areas where there is a high inherent risk such as Health and Safety
- that risks around projects and partnerships must be effectively captured and communicated within the risk management framework of the organisation to ensure that a holistic approach to risk management is embedded
- that effective risk management will help improve the delivery of the outcomes identified in the Southend 2050 programme by directing finite Council resources to where they can achieve the most, whilst exploiting opportunities to achieve outcomes via more innovative means.

These views are endorsed by the increased focus on the importance of governance frameworks within public sector bodies and that the Council has a statutory responsibility to have in place arrangements for managing risks, as stated in the Accounts & Audit Regulations 2015:

“The relevant body shall be responsible for ensuring that the financial management of the body is adequate and effective and that the body has a sound system of internal control which facilitates the effective exercise of that body’s functions and which includes the arrangements for the management of risk.”

The Risk Management Policy Statement and Strategy provides the foundation on which robust risk management activity, supporting the efficient and effective achievement of outcomes and delivery of services, will be embedded within business processes and contribute to the effectiveness of the governance framework.

More detail to support and guide the organisation in successfully embedding Risk Management will be provided within the guidance that will accompany this strategy.

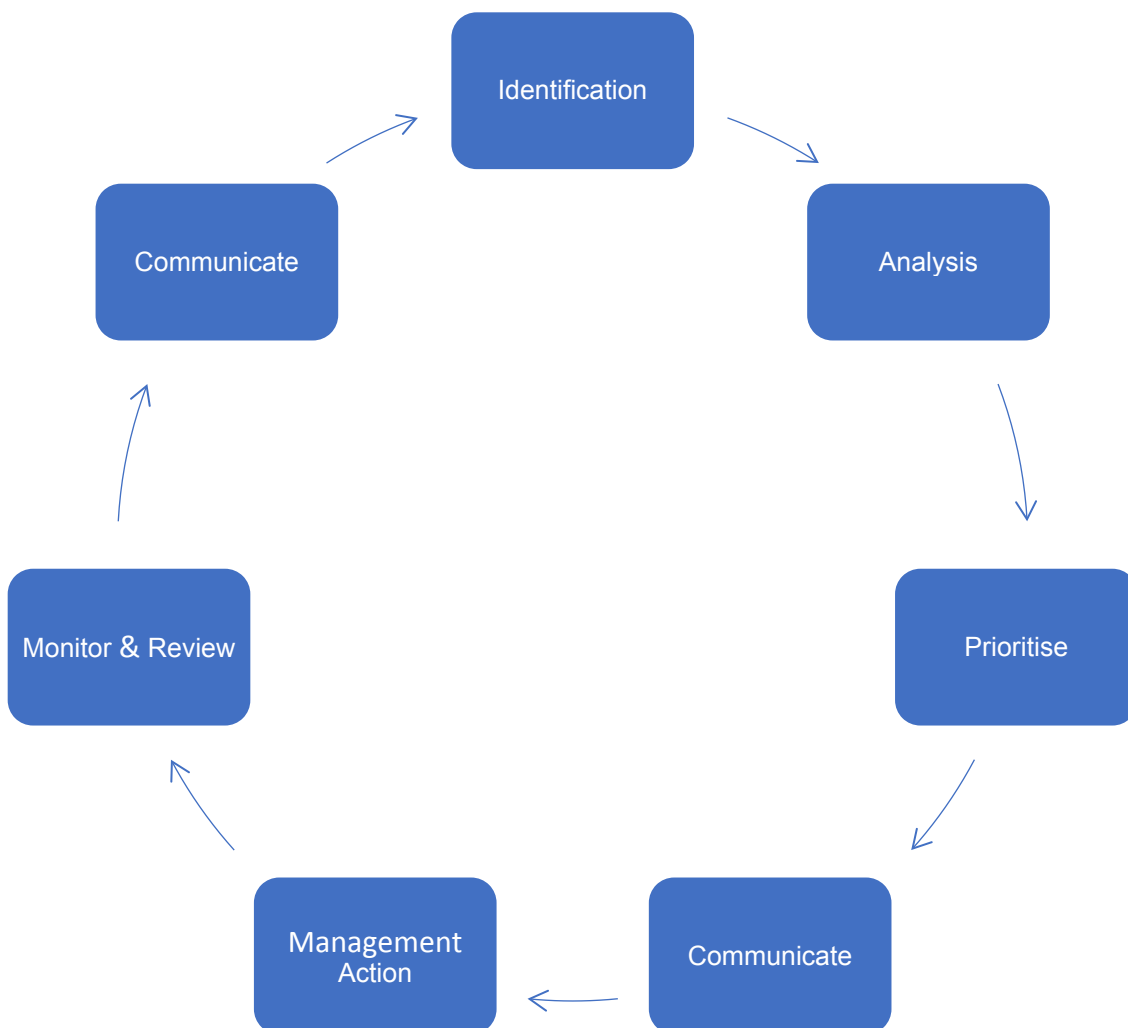
An action plan, covering the planned duration of the Strategy, has been developed to implement the strategy and further embed Risk Management into the governance framework of the organisation (Appendix 2).

Definition of Risk

The definition of risk used within the Council is that **RISK** is 'The chance of something happening that will have an impact (negative = threat or positive = opportunity) on the Council's ability to successfully deliver its approved outcomes. This includes external and internal, risks and opportunities'.

RISK MANAGEMENT is therefore the process by which risks are identified, analysed, prioritised, managed and monitored / reviewed. The Council has determined two clear points in the cycle where communication needs to be considered.

FIG 1: Risk Management Cycle



The approved methodology will be outlined within the guidance to support Management, however the high level approach is outlined in paragraphs below.

The activity to **IDENTIFY** risk is most effective when aligned to strategic, operational and project planning processes focused on the achievement of outcomes. In the context of the Southend 2050 programme risk will be identified against the themes and outcomes identified within the Council's ambition.

The Council's methodology for risk **ANALYSIS** is for the **likelihood** of the risk materialising, and the **impact**, should it materialise, to be scored using a defined criteria and scored on a four by four grid.

Guidance that supports the implementation of this strategy provides criteria to promote consistency of evaluation of risk across the organisation.

A template Risk Register is in place for the Corporate Risk Register which is supported by the Pentana system. Templates used for all risk registers will be refined and agreed by December 2019 as part of implementing this strategy. The aim will be to ensure consistency across the organisation in how risk is captured and communicated but also ensure that the templates are fit for purpose to support a streamlined approach.

A summary table is included here for information to assist in risk **ANALYSIS**. More detailed guidance is included within the Risk Management Toolkit.

| Likelihood | | | Impact | | |
|------------------|----------|--------------------------------------|---|--|--------|
| Score 1-4 | % chance | Time Frequency | Score 1-4 | Disruption to Services <i>Residents affected or aware</i> | Budget |
| 1 Unlikely | < 25% | Once in <5 years | 1 Negligible | Minor disruption to services <i>Up to 5%</i> | >1% |
| 2 Likely | 25 -50% | Once in < 3 years | 2 Material | 1-2 weeks <i>Up to 10%</i> | >5% |
| 3 Very Likely | 50-75% | could materialise next 18-24 months | 3 Severe /Significant Opportunity | Up to one month <i>Up to 25%</i> | 5-10% |
| 4 Almost Certain | >75% | could materialise within 6-12 months | 4 Catastrophe / Exceptional Opportunity | 1 – 3 month <i>Up to 50%</i> | 10-20% |

Consistency is also increased through the challenge mechanisms that exist within the governance structure which are documented in the delivering the strategy section. These challenge mechanisms are outlined in the appendices of this strategy (see Appendix 1).

Plotting the risks visually can help with prioritisation and also challenge i.e. when risks are reviewed in relation to other risks also being reported within the organisation. The grid below is used to present the relative importance of risks.

Risk Matrix

Risk tolerance level – Risks above this level will need particular resources and focus

I
M
P
A
C
T

| | | | | |
|--|---------------|---------------|--------------------|---------------------|
| Catastrophic / exceptional opportunity | 4 | 8 | 12 | 16 |
| Severe / significant opportunity | 3 | 6 | 9 | 12 |
| Material | 2 | 4 | 6 | 8 |
| Negligible | 1 | 2 | 3 | 4 |
| | Unlikely <25% | Likely 25-50% | Very Likely 50-75% | Almost Certain >75% |

Risk acceptance level (activity below which attracts minimum effort and resources)

LIKELIHOOD

Risk Ratings: 1 – 2 = low risk (Green) / 3 – 10 = medium risk (Amber) / 12 – 16 – high risk (Red)

In assessing a risk there are three ratings to be confirmed from the analysis of the risk.

The **Inherent Risk** Score – the level of risk before any mitigations have been applied.

The **Residual Risk** Score – taking into account the mitigations currently in place and the effectiveness of those implemented mitigations.

The **Target Risk Score** – the level at which the risk will fall within the Council's appetite and be accepted.

Decisions regarding target risk will be driven by the approved **Risk Appetite** This is the amount of risk that the Council is willing to seek or accept in the pursuit of its objectives.

Risk appetite will vary from person to person and is influenced by the type of risk. Guidance will be provided to Management and mechanisms within the process and procedures are designed to challenge and as a result increase consistency of decisions regarding risk across the Council. This will be reported to Cabinet twice a year, and annually the effectiveness of these mechanisms will be considered and assurances provided to Audit Committee to assist with their Annual Report to Council.

The **Risk Tolerance** of the organisation is the boundaries of risk taking outside which the Council is not prepared to venture in the pursuit of its long-term objectives. Effective communication regarding risk is essential to ensuring that the risk appetite being applied is ensuring risks are managed within the approved tolerance level.

The Risk Appetite and Tolerance of the organisation will be considered annually as part of the planned annual review of the framework, and changes to procedures and guidance made as required.

The **PRIORITISATION** of risks will be dependent of the outcome of the analysis stage and the gap between the residual and target risk ratings.

When taking decisions regarding the appropriate action to manage a risk consideration will be given to whether it is the likelihood or impact that we seek to reduce.

At this stage it may be necessary for **COMMUNICATION** with other individuals, teams, groups or boards. Others may need to understand the risk that is being managed, or their role in the control environment that needs to be in place.

Risks can be **MANAGED** by:

- **Treating** – management action / control to bring within risk appetite or to ensure that the opportunities available are being optimised
- **Transferring** – passing to a third party, usually via a contract i.e. insurance – this would bring the activity within the council's appetite and overall tolerance level
- **Tolerating** – accepting the current level of risk, because it is within the council's defined appetite to do so and/or the cost of mitigations to reduce it further outweigh benefits to be gained in terms of affecting the likelihood or impact
- **Terminating** – ceasing the activity – usually because the risk exceeds the Council's appetite or moves the overall level of risk over its tolerance for risk and/or the cost of mitigations to rectify this far exceeds the resources available.

Risks and their corresponding action plans need to be periodically **REVIEWED AND MONITORED** to ensure changes are recognised and captured. The frequency of review should not be arbitrary, focus should be directed based on three factors:

- 1) The level of risk, more frequent attention to those of most significance to outcomes
- 2) Those risks where deadlines for actions are due, it is important to ensure actions are completed as planned and that they have had the expected effect on the risk rating
- 3) Risks where the Residual and Target risk ratings are furthest apart, as these are the risks where the council is most exposed and greatest action is required to move to within appetite.

There will be an expectation that risk registers are formally reviewed at least quarterly throughout the financial year.

Efficiency can be built into this process by ensuring robust assurances are in place regarding the materialisation of risk indicators or with regards to the design of the control environment. These assurances exist within the Council in many forms, this includes but is not limited to performance data, feedback, reviews, inspections and internal audits. Where gaps in assurances are noted then Management may not have reliable information with which to manage risk.

As risks are reviewed it may be necessary to **COMMUNICATE** the risk to others. If management actions have failed to reduce risk then it may need to be escalated. If the risk has changed then despite actions taken working the risk may still have increased and need to be escalated. Risks that become deemed to be managed to within appetite may be removed from the corporate risk register and included on a more operational risk register level, for on-going monitoring.

AIMS AND OBJECTIVES

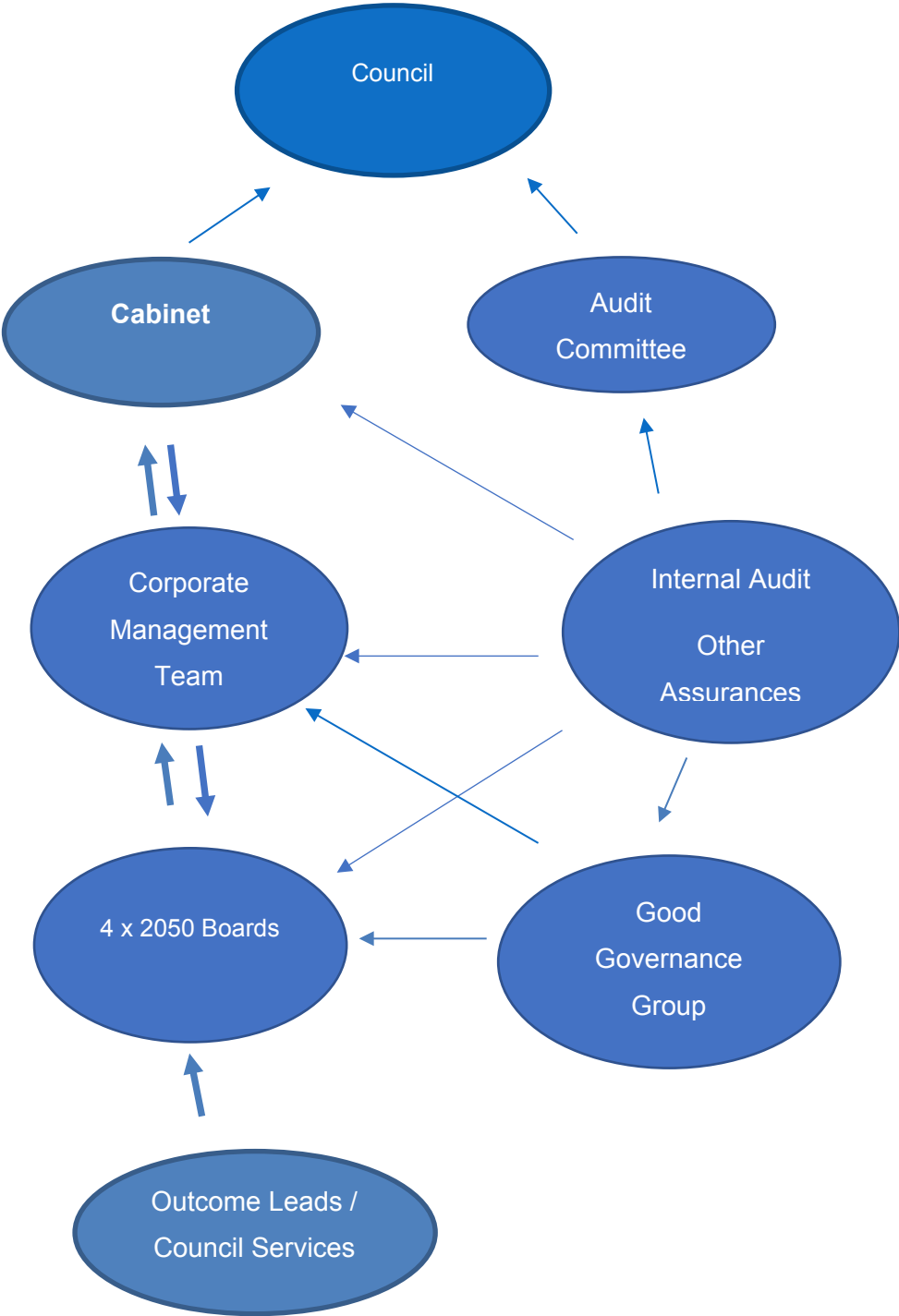
The Council's Risk Management aims and objectives, for the period of this Strategy, are as follows:

- To ensure that actions taken to maximise opportunities and minimise the likelihood of risks crystallising, and / or reducing the impact of consequences should risks crystallise, are in accordance with the Council's defined appetite and tolerance
- To further embed robust risk management into the culture of the Council in line with the approved policy, supporting procedures and good practice
- To ensure that the Risk Management process including effective reporting arrangements to senior Management and Members remain fit for purpose, optimising the efficiency of resources input.

How these objectives will be achieved is outlined within the Delivering the Strategy section below.

DELIVERING THE STRATEGY

The diagram below outlines the governance structure with regards risk management.



Appendix 1 outlines the roles and responsibilities with regards Risk Management in the Council. The effective delivery of the strategy will be reliant on fulfilment of the respective roles and responsibilities.

An action plan is in place to ensure implementation of the approved policy and strategy. This can be found at **Appendix 2**. From 2019/20 there is an acknowledgement that the activity will be supported by the Head of Internal Audit with other risk resources, and that the procedures will need to continue to develop and evolve as the governance around the 2050 programme evolves, until this becomes embedded.

A timetable for reporting cycles has been included as **Appendix 3** for the financial year 2019/20. This will be updated and communicated to key stakeholders annually as part of the annual review of the risk management arrangements.

A guidance document will be created to support officers in applying the requirements of the policy and strategy into their day to day roles and responsibilities. This will be finalised and approved by December 2019.

| Group / Individual | Role / Responsibility |
|---|--|
| Cabinet | <ul style="list-style-type: none"> • To have regard to the risks faced by the council within the Cabinet decision making process • Periodically review and challenge the Corporate Risk Register • Endorse the Council's Risk Management Policy Statement and Strategy. |
| All Councillors | <ul style="list-style-type: none"> • Support and promote risk management • Consider the risks involved in any key decisions made. |
| Councillor Theme / Outcome Leads | <ul style="list-style-type: none"> • Support the development and have a shared understanding of the risk registers that relate to their allocated theme / outcome. |
| Audit Committee | <ul style="list-style-type: none"> • To assure themselves that the Risk Management Framework is operating effectively and in accordance with the approved Policy and Strategy • To provide independent assurance to Cabinet and Council on the above • Seek assurances that action is being taken on risk related issues identified by auditors and inspectors. |
| Chief Executive and Corporate Management Team | <ul style="list-style-type: none"> • To ensure that the corporate risk register reflects those organisational risks that may prevent it delivering on the 2050 ambition • Support and promote risk management throughout the council • To oversee the development / review of the council's Risk Management Strategy / Framework • To ensure engagement in risk and control mechanisms across their respective service areas. |
| Head of Internal Audit (Officer Champion for Risk) | <ul style="list-style-type: none"> • Facilitating the link across risk management activity at the corporate level • Managing resources to support risk management in the organisation at the operational level • Attending CMT quarterly strategic forward looking meetings • Identifying the resources to deliver the action plan (appendix 2) and confirming to CMT and Audit Committee they are in place. |
| S2050 Theme Leads | <ul style="list-style-type: none"> • Champion and ensure that risk management is implemented across the five themes and 23 outcomes • Identify relevant lead officers / risk owners as appropriate • To ensure that Members are briefed on significant risks that fall within their theme / outcome and actions to address these • Consider cross cutting, joint working and risks within partnership working • Escalate risks as appropriate to CMT / Corporate Risk Register. |
| Good Governance Group | <ul style="list-style-type: none"> • Challenge the Corporate Risk Register quarterly • Focus their agenda on gaps in controls and / or assurances |
| S2050 Outcome Leads | <ul style="list-style-type: none"> • To embed risk management into their outcome and escalate risks as required. |
| Risk Champions | <ul style="list-style-type: none"> • To support the continued development of risk management by embedding risk management in the running of their respective board/service and acting as a point of contact to provide support and information as appropriate. |

| Group / Individual | Role / Responsibility |
|--------------------------|---|
| Internal Audit | <ul style="list-style-type: none"> • To offer independent, objective assurance and advice on risk management activity • To undertake an audit of risk management arrangements and make recommendations on actions to be considered • To provide assurance on the effectiveness of controls, including annual assessment of the council's risk management and internal control mechanisms as part of the Annual Governance Statement. |
| Risk Management Function | <ul style="list-style-type: none"> • To ensure that the Risk Management Framework, including the Policy Statement, Strategy and guidance, are kept up to date, reflect best practice and are relevant to the organisation • To provide support on risk management across the council • To co-ordinate the reporting of the corporate risk register to senior officers and Councillors and provide advice and challenge as appropriate, including the tracking of action plans in the risk register • To support the identification of and analyse key new and emerging risks and report to CMT for consideration (horizon scanning) • Support communication of the risk management strategy and process, and update as appropriate, across the council through risk reviews and training sessions • Advise on possible actions that may be required in respect of business change initiatives • Ensuring there is a robust framework of assurances shared within the council. For example ensuring there is periodic consideration of insurance management information reports and other risk focused performance data, and take forward any identified initiatives arising from identifying incidents that can add value to the business and avoid loss control • Promoting risk management awareness. |
| All Employees | <ul style="list-style-type: none"> • To understand the risks that relate to their role and activities and their role in reporting on and managing these • To report new or emerging risks in a timely manner. |

| Ref | Implementation Action Plan | Estimated Timing by |
|-----|---|---------------------|
| 1 | General communications to the organisation following approval of the Policy Statement and Strategy | September 2019 |
| 2 | Attendance at four 2050 Governance Boards to capture programme / corporate risks Identification of Risk Champions | October 2019 |
| 3 | Attendance at Good Governance Group to workshop corporate risks and procedures | October 2019 |
| 4 | Attendance at CMT to propose risk management procedures and seek approval for operational guidance documents | November 2019 |
| 5 | Attendance at Directorate Management Team Meetings to promote risk management and new approach | December 2019 |
| 6 | Refresh of Corporate Risk Register | December 2019 |
| 7 | Attendance at service team meetings to promote new approach | March 2020 |
| 8 | Meetings with outcome leads / groups to workshop risks | March 2020 |
| 9 | Refresh of Corporate Risk Register | March 2020 |
| 10 | Update and refresh of this action plan for 2020/21 as part of the Annual Review of Risk Management | May 2020 |
| 11 | Independent review of Risk Management for inclusion in Annual Report and Head of Internal Audit Opinion. To manage conflict of interest for Head of Audit. | May 2020 |

| Dates | Reporting Action Required |
|---------------|--|
| October 2019 | 2050 Governance Boards to capture programme / corporate risks |
| October 2019 | Good Governance Group to workshop corporate risks and procedures |
| December 2019 | CMT to propose risk management procedures |
| December 2019 | CMT update and Corporate Risk Register |
| January 2020 | Cabinet update and Corporate Risk Register |
| February 2020 | CMT update and Corporate Risk Register |
| May 2020 | Good Governance Group update and Corporate Risk Register |
| May 2020 | CMT update and Corporate Risk Register |
| July 2020 | Cabinet update and Corporate Risk Register |

Counter Fraud, Bribery and Corruption Policy and Strategy

VERSION CONTROL SHEET

| | |
|--------------------------|---|
| Title: | Counter Fraud, Bribery and Corruption Policy and Strategy |
| Purpose: | To advise council workers and suppliers on what fraud, bribery and corruption is, how to identify it and report it. |
| Owner: | Counter Fraud & Investigation Directorate |
| Approved by: | Corporate Management Team – 07/08/2019 Cabinet – 17/09/2019 |
| Date: | Approved – 17/09/2019 Implemented – 18/09/2019 |
| Version Number: | 2.2 |
| Status: | Draft |
| Review Frequency: | Bi-annually |
| Next Review Date: | September 2021 |

| Change History | | |
|----------------|--|---|
| Date | Change Details | Approved by |
| Nov 2018 | Revision of formatting and reporting methods, legislative changes. | Joe Chesterton, Strategic Director (Finance & Resources) |
| August 2019 | Revision of formatting and reporting methods, legislative changes. | Joe Chesterton, Strategic Director (Finance & Resources) John Williams, Strategic Director (Legal & Democratic Services) |

Policy Statement

Southend-on-Sea Borough Council is serious about protecting the public money we are charged with to protect. We take a strong stance against those who seek to commit fraud against the council.

It is an unfortunate reality that Southend-on-Sea Borough Council, like any large organisation, is not immune from fraud, bribery and corruption from both those outside the organisation and the few who may work here and commit crime.

Cases of internal fraud are extremely rare and we have a strong framework of policies and controls in place to detect any risks, supported by our Internal Audit Service and Counter Fraud & Investigation Directorate.

This policy sets out what the council will do to make it the most difficult environment for fraud to occur and the responsibility on everyone in the council to find fraud and report it.

Fraud in councils can happen anywhere. No team or department is immune. As a council we spend around £520m annually. International standards say that about 3% of that spending will be lost due to fraud and corruption. That equates to £15m, every year.

It is important that we look after our resident's money and make sure no one misuses it. It is incumbent on all of us in the council to report any suspicions we may have and support the Internal Audit and Counter Fraud services in their work.

Alison Griffin

Chief Executive & Town Clerk

Contents

| | |
|---|-----------|
| 1. Introduction..... | 3 |
| 2. What is Fraud?..... | 3 |
| 3. How is fraud committed against the Council? | 4 |
| 4. What is bribery and corruption? | 5 |
| 5. What do I do if I suspect fraud, bribery or corruption? | 6 |
| 6. What does the Council do with cases of suspected fraud? | 6 |
| 7. Whistleblowing | 7 |
| 8. Information Sharing | 7 |
| 9. Monitoring Delivery | 8 |
| Appendix 1: Roles & Responsibilities..... | 9 |
| Appendix 2: Key Contacts..... | 11 |
| Appendix 3: Fraud Legislation..... | 12 |
| Appendix 4: Bribery & Corruption Legislation..... | 14 |

1. Introduction

- 1.1 As a local authority Southend-on-Sea Borough Council (the Council) is responsible for delivering key frontline services such as maintaining roads, keeping our borough clean and green, educating our children and young adults as well as supporting the vulnerable in health and social care support.
- 1.2 We deliver these services with the £520m of public money we have in our budget. Criminals do and will continue to seek to take that money from the Council. Criminals can come in all forms from services users, to suppliers and the colleagues sitting next to us.
- 1.3 The way to beat those who seek to take the public's money is to make sure our systems and controls in place are strong, and then consistently implement them. This means all of the procedures we have as teams are robust and auditable, so we can prevent fraud and identify possible concerns.
- 1.4 This policy sets out what fraud, bribery and corruption is, how you can spot it and what to do if you suspect it.
- 1.5 Every council worker and our partners are responsible for following this policy and reporting their suspicions to our Head of Internal Audit and Counter Fraud & Investigation Directorate.
- 1.6 As council workers we are public officials who must all follow the seven Principles of Public Life, also known as the Nolan Principles. These are:

1. Selflessness

Holders of public office should act solely in terms of the public interest.

2. Integrity

Holders of public office must avoid placing themselves under any obligation to people or organisations that might try inappropriately to influence them in their work. They should not act or take decisions in order to gain financial or other material benefits for themselves, their family, or their friends. They must declare and resolve any interests and relationships.

3. Objectivity

Holders of public office must act and take decisions impartially, fairly and on merit, using the best evidence and without discrimination or bias.

4. Accountability

Holders of public office are accountable to the public for their decisions and actions and must submit themselves to the scrutiny necessary to ensure this.

5. Openness

Holders of public office should act and take decisions in an open and transparent manner. Information should not be withheld from the public unless there are clear and lawful reasons for so doing.

6. Honesty

Holders of public office should be truthful.

7. Leadership

Holders of public office should exhibit these principles in their own behaviour. They should actively promote and robustly support the principles and be willing to challenge poor behaviour wherever it occurs.

2. What is Fraud?

- 2.1 In this policy 'fraud' is used as shorthand for any criminal offence where money or assets belonging to the Council can be lost. It includes theft, fraud, burglary and other deception offences such as corrupt practices by those who work for us or suppliers.
- 2.2 Fraud is where a person is dishonest in their actions in order to cause a loss to the Council or expose the Council to a potential loss. It also includes where a person causes a chain of events by doing **or** not doing something, that causes **or** exposes the Council to a loss.
- 2.3 Any of the actions described above are criminal offences and can result in imprisonment.

3. How is fraud committed against Council?

Applying for Services / Making a Declaration

- 3.1 The Council provides hundreds of different services to the public we serve. Unfortunately there is a small minority of those who seek to take advantage of those services. This could be by a person embellishing their circumstances, making something up completely or purposefully not declaring something.
- 3.2 In the Council's welfare support services such as Social Care, Housing and Essential Living Fund, this could be a person not being honest about their needs, what their financial status is or what they will be using the services for. It may be a person acting on the service user's behalf that is being dishonest in order to benefit them.
- 3.3 In each of these examples the frauds are denying the legitimate use of Council funds for those who are in need.

Suppliers / Providers

- 3.4 The highest risk to the public sector is from its supply chain. A Council is a business making regular and sometimes large financial transactions with our suppliers and providers in order to deliver our services.
- 3.5 Some unscrupulous suppliers, or staff working in supplier companies, may seek to take advantage of our payment systems and processes.
- 3.6 Fraud in this area can be committed where suppliers submit false or 'erroneous' invoices or other requests for payment. Suppliers may also be dishonest in how they are delivering the services or goods we have asked them for. They may be poor quality or not supplied at all.
- 3.7 Staff that deal with our suppliers and providers must ensure that the Council is getting what it has paid for. The Council's Corporate Procurement Team is experienced in letting and managing contracts and applying the right controls when sourcing goods, works and services.

Did you know?

In 2014, the Council prosecuted a Foster Carer who stole £5,500 from a child in their care.

Council Worker Fraud

- 3.8 Like any large employer employing thousands of people, there will always be a small minority of people who seek to commit fraud or allow fraud to take place.
- 3.9 Fraud in this area can be staff who take unauthorised absences, such as:
- Claiming 'flexi time' when they haven't accrued any
 - Claiming to be working from home when they are not
 - Claiming to be working in the field but going home early / starting later.
- 3.10 Payroll or expenses fraud can also be committed by Council workers. For example, staff falsely claiming overtime for hours they have not worked or mileage or subsistence for expenses they have not incurred.
- 3.11 It is therefore important for all staff to follow the Council's procedures, particularly those staff in management positions authorising such claims or transactions, as well as colleagues who may notice irregularities.

Did you know?

The impact if all staff falsely worked half an hour less per week would effectively be a cost to the Council of £130k every year.

4. What is bribery and corruption?

- 4.1 As public servants, all workers in the Council are in a privileged position to serve the public of Southend-on-Sea. That responsibility comes with a significant amount of trust and confidence in how we conduct ourselves.
- 4.2 It has always been a criminal offence for anyone working at the council to receive gifts or hospitality where the person giving the gift or hospitality is seeking to induce us to, or reward us for doing something for their, or somebody else's benefit.
- 4.3 This type of corruption has been depicted in many different films and fictional stories since time began. Examples have seen cases of criminals:
- seeking to build a house that would normally be rejected by planners
 - wanting the Council to 'look the other way' for parking fines or other enforcement responsibilities.
- 4.4 This type of criminality is the most serious type of dishonesty.
- 4.5 Those who act corruptly or offer themselves to receive gifts or hospitality to feed this criminality bring the Council and their colleagues in to disrepute.

5. What do I do if I suspect fraud, bribery or corruption?

- 5.1 The Counter Fraud & Investigation Directorate (CFID) is responsible for dealing with any cases of suspected criminality described in this policy, **not the police**.
- 5.2 It is the responsibility of everyone working here to look for and report any possible fraud taking place. You **do not** have to speak to a manager before reporting your suspicions.
- 5.3 If you see any of the suspicious activity linked to fraud **you should**:
- △ Not tell the person that you have any suspicions about them
 - △ Take copies of any records that could help to a secure location
 - △ Telephone a member of the CFID team right away on **03000 999111 (24/7)**
 - △ Follow the instructions given by the CFID team.

6. What does the Council do with cases of suspected fraud?

- 6.1 The Council has a dedicated team of professionally trained and accredited investigation officers who fully investigate instances of suspected fraud. The CFID team work around the clock, anywhere in the UK, utilising powers to arrest persons, search their premises and seize their assets to take back what the Council has lost.
- 6.2 In cases where there may be a proven case of fraud the Council's Legal Services has dedicated Criminal Prosecutors who apply the Code for Crown Prosecutors. This code is used by a lawyer to decide, independently, whether:
- there is sufficient evidence of a crime
 - it is in the public interest to prosecute those responsible.

Did you know?

Since 2014, the Council has recovered £552k from fraudsters.

- 6.3 CFID also has a dedicated Criminal Finances Unit that is accredited by the National Crime Agency to present cases to a Judge where necessary to obtain consent to pursue actions requiring that approval, and confiscate any criminal proceeds.
- 6.4 The Council will always publicise cases of proven fraud in the media to act as a deterrent and encourage people to come forward to report fraud.
- 6.5 CFID share all the allegations they have received and the work that they have done to investigate those allegations with the Executive Director (Finance & Resources) and the Head of Internal Audit on a monthly basis.

7. Whistleblowing

- 7.1 The Council is committed to providing the highest quality service to our residents, businesses and visitors to Southend-on-Sea. Maintaining the full trust and confidence in the way the Council manages our services and resources is essential. Our priority is making sure those in need and vulnerable are provided for safely, effectively and in accordance with best practice.
- 7.2 The Council's Whistleblowing Policy is intended to encourage and enable workers to raise serious concerns. Council workers reporting concerns this way are afforded certain rights and protection through legislation enacted under the Public Interest Disclosure Act 1998.
- 7.3 Workers who report concerns will be supported and protected from reprisals. Everything possible will be done to protect their confidentiality. They will be advised of the action that has been taken by the person to whom they reported their concerns.
- 7.4 Management are responsible for reporting all allegations received from whistleblowing under the confidential reporting code to the Monitoring Officer. The Monitoring Officer will refer the allegations relating to suspected fraud, money laundering, bribery and corruption to the Counter Fraud & Investigation Directorate for investigation. All such cases should be recorded in a register maintained by the Monitoring Officer.
- 7.5 CFID will deal with the matter promptly, efficiently and in accordance with the law, involving such outside agencies as appropriate (including the police). Where a service provider employee is involved, the supplier will be informed where appropriate in liaison with the Executive Director (Finance & Resources) and CFID.

8. Information Sharing

- 8.1 As a responsible data controller, the Council always ensures that personal data we hold is safeguarded in accordance with the Data Protection Act 2018 and the General Data Protection Regulation.
- 8.2 The Council will use data to ensure that we are protected from any cases of suspected fraud, bribery or corruption as well as money laundering and identify those involved.
- 8.3 Any workers contacted by the CFID, Internal Audit or Legal Services as part of a criminal investigation must provide any Council data held in any form (paper or electronically). Council workers must not tell anyone that they have been asked for any material for an investigation, unless permitted to by the CFID, Internal Audit or Legal Services.
- 8.4 Any concerns workers may have about releasing information should be directed to the Assistant Director for Fraud & Investigation, Head of Internal Audit, Strategic Director (Finance & Resources) or Strategic Director (Legal & Democratic Services).

9. Monitoring Delivery

- 9.1 The CFID leads the Council's fight against fraud and economic crime, including bribery and corruption. The team reports quarterly to the Council's Corporate Management Team and Audit Committee on its work to tackle the problem and its performance in delivering this Strategy.

Expected Behaviour

The Council requires all staff and Councillors to act honestly and with integrity at all times and to safeguard the resources for which they are responsible. Fraud is an ever-present threat to these resources and hence must be a concern to all staff and Councillors. The purpose of this statement is to set out specific responsibilities with regard to the prevention of fraud.

Section 151 Officer (Executive Director (Finance & Resources)) is responsible for:

- Proper administration of the authority's financial affairs
- Reporting to Councillors and External Audit if the Council, or one of its representatives makes, or is about to make, a decision which is unlawful, or involves illegal expenditure or potential financial loss (Local Government Finance Act 1988 s.114)

Monitoring Officer is responsible for:

- Reporting on contraventions or likely contraventions of any enactment or rule of law
- Report on any maladministration or injustice where the Ombudsman has carried out an investigation
- Receiving copies of whistleblowing allegations of misconduct
- Promoting and maintaining high standards of conduct through and with the support of the Standards Committee
- Advice on vires (legality) issues, maladministration, financial impropriety, probity and policy framework and budget issues to all Councillors

Managers are responsible for:

- Maintaining internal control systems and ensuring that the authority's resources and activities are properly applied in the manner intended
- Identifying the risks to which systems and procedures are exposed
- Developing and maintaining effective controls to prevent and detect fraud
- Ensuring that controls are being complied with, including making sure their staff are performing well and meeting council policies and procedures.

Individual members of staff are responsible for:

- Their own conduct and for contributing towards the safeguarding of corporate standards (including declarations of interest, gifts & hospitality, private working, whistleblowing etc.)
- Acting with propriety in the use of official resources and in the handling and use of corporate funds, such as when dealing with contractors and suppliers
- Reporting details immediately to the Counter Fraud & Investigation Directorate if they suspect that a fraud, theft, bribery, corruption or money laundering has been committed, or see any suspicious acts or events

Southend-on-Sea Borough Council
Counter Fraud, Bribery and Corruption Policy and Strategy
Appendix 1: Roles & Responsibilities

Internal Audit is responsible for:

- The independent appraisal of control systems
- Reporting to the Corporate Management Team and the Audit Committee on the council's governance framework
- The implementation of an annual audit plan to include identification of fraud risks to the Counter Fraud & Investigation Directorate

Counter Fraud & Investigation Directorate is responsible for:

- The investigation into allegations of any money laundering, fraud, bribery, theft, corruption and related offences committed against the authority
- Reporting of persons for consideration of prosecution (or the application of an alternative sanction)
- All action under the Proceeds of Crime Act 2002 and Criminal Justice Act 1988 in respect of financial investigation, restraint, detention, forfeiture and confiscation
- The co-ordination of participation in the National Fraud Initiative (NFI)
- Providing Counter-Fraud, Money Laundering, Theft, Bribery & Corruption Awareness
- Taking redress from offenders under criminal and civil law
- Referring any matters to & receiving information and intelligence from all law enforcement agencies (Police, HMRC, Home Office etc) where appropriate.

External Audit has specific responsibilities for:

- Reviewing the stewardship of public money
- Considering whether the Council has adequate arrangements in place to prevent fraud and corruption
- Signing off the annual accounts of the authority

Councillors are each responsible for:

- Their own conduct
- Contributing towards the safeguarding of corporate standards, as detailed in the Members' Code of Conduct

Southend-on-Sea Borough Council
Counter Fraud, Bribery and Corruption Policy and Strategy
Appendix 2: Key Contacts

| Contact | Details |
|---|---|
| Counter Fraud & Investigation Directorate | 9 th Floor, Civic Centre, Victoria Avenue, Southend-on-Sea, SS2 6EN Tel: 03000 999 111 E-mail: counterfraud@southend.gov.uk Web: southend.gov.uk/fraud |
| David Kleinberg Assistant Director for Fraud & Investigation | Tel: 03000 999 111 E-mail: davidkleinberg@southend.gov.uk |
| Joe Chesterton Strategic Director (Finance & Resources) <i>(s.151 Chief Finance Officer)</i> | 10 th Floor, Civic Centre, Victoria Avenue, Southend-on-Sea, SS2 6EN Tel: 01702 215200 E-mail: joechesterton@southend.gov.uk |
| John Williams Strategic Director (Legal and Democratic Services) <i>(Monitoring Officer)</i> | 2 nd Floor, Civic Centre, Victoria Avenue, Southend-on-Sea, SS2 6EN Tel: 01702 215102 E-mail: johnwilliams@southend.gov.uk |
| Andrew Barnes Head of Internal Audit | 9 th Floor, Civic Centre, Victoria Avenue, Southend-on-Sea, SS2 6EN Tel: 07827 348375 E-mail: andrewbarnes@southend.gov.uk |
| Protect <i>(Independent charity for whistleblowing, providing free independent legal advice)</i>  | CAN Mezzanine, 7-14 Great Dover Street, London SE1 4YR Tel: 020 3117 2520 E-mail: whistle@protect-advice.org.uk Web: pcaw.org.uk |

1 Fraud

- 1.1 The Fraud Act 2006 introduced the first statutory definition of fraud whereby:

“A person is guilty of fraud if he is in breach of any of the sections listed in subsection (2) (which provide for different ways of committing the offence).

Fraud can be committed by:

- a) section 2 (Fraud by False Representation),*
- b) section 3 (Fraud by Failing to Disclose Information), and*
- c) section 4 (Fraud by Abuse of Position). “*

Fraud by false representation

A fraud will be committed if a person dishonestly makes a false representation and when doing so intends to make a gain or cause loss (or a risk of loss) to another.

Fraud by failing to disclose information

A fraud will be committed if a person dishonestly fails to disclose information where there is a legal obligation to do so and when doing so intends to make a gain or cause loss (or a risk of loss) to another.

Fraud by abuse of position

A person will commit fraud if he occupies a position in which he is expected to safeguard, or not act against, the financial interests of another person and he dishonestly abuses that position; and in doing so intends to make a gain or cause loss (or a risk of loss) to another.

2 Theft, Burglary and Robbery

- 2.1 A person is guilty of **theft** if they dishonestly appropriate property, belonging to another, with the intention of permanently depriving the other of it.
- 2.2 Theft includes where someone takes something “and uses it as their own”.
- 2.3 A person is guilty of **robbery** if they steal, and immediately before or at the time of doing so, and in order to do so, they use force on any person or put or seek to put any person in fear of being then and there subjected to force.
- 2.4 A person is guilty of **burglary** if they enter any building or part of a building as a trespasser and with intent to steal anything in the building or part of a building in question, of inflicting on any person therein any grievous bodily harm; or having entered any building or part of a building as a trespasser they steal or attempt to steal anything in the building or that part of it or inflicts or attempts to inflict on any person therein any grievous bodily harm.

1 Bribery

- 1.1 A bribe is *“a financial or other advantage that is offered or requested with the intention of inducing or rewarding the improper performance of a relevant function or activity, or with the knowledge or belief that the acceptance of such an advantage would constitute the improper performance of such a function or activity.”*
- 1.2 The types of offending relating to bribery are:
- 1.2.1 **Bribery:** Giving or receiving something of value to influence a transaction dishonestly makes a false representation.
 - 1.2.2 **Illegal gratuity:** Giving or receiving something of value after a transaction is completed, in acknowledgment of some influence over the transaction.
 - 1.2.3 **Extortion:** Demanding a sum of money (or goods) with a threat of harm (physical or business) if demands are not met.
 - 1.2.4 **Conflict of interest:** Where a worker has an economic or personal interest in a transaction.
 - 1.2.5 **Kickback:** A portion of the value of the contract demanded / provided as a bribe by an official for securing the contract.
- 1.3 The Bribery Act 2010, which came into force on 1st July 2011, introduced four primary offences in a single piece of legislation with all previous statutes being repealed.
- 1.3.1 Section 1: Offences of bribing another person, where:
 - (a) *a person offers, promises or gives a financial or other advantage to another person, and*
 - (b) *intends the advantage to:*
 - (i) *induce a person to perform improperly a relevant function or activity, or*
 - (ii) *reward a person for the improper performance of such a function or activity.*
 - 1.3.2 Section 2: Offence relating to being bribed.
 - 1.3.3 Section 6: Bribery of foreign public officials.
 - 1.3.4 Section 7: Failure by a commercial organisation to prevent bribery.
- 1.4 Under the Bribery Act, an organisation has a defence if it can show that it has adequate bribery prevention procedures in place. The Ministry of Justice guidance¹ on the Bribery Act 2010, explains what needs to be in place to rely on this defence:
- 1.4.1 **Proportionality:** An organisation’s procedures to prevent bribery by persons associated with it are proportionate to the bribery risks it faces and to the nature, scale and complexity of the organisation’s activities. They are also clear, practical, accessible, effectively implemented and enforced.
 - 1.4.2 **Top Level Commitment:** *Those at the top of an organisation are in the best position to ensure their organisation conducts business without bribery. We want to show that we have been active in making sure that our staff (including*

¹ <http://www.justice.gov.uk/downloads/legislation/bribery-act-2010-quick-start-guide.pdf>

Southend-on-Sea Borough Council
Counter Fraud, Bribery and Corruption Policy and Strategy
Appendix 4: Bribery and Corruption Legislation

any middle management) and the key people who do business with us and for us understand that we do not tolerate bribery.

- 1.4.3 **Risk Assessment:** The organisation assesses the nature and extent of its exposure to potential external and internal risks of bribery on its behalf by persons associated with it. The assessment is periodic, informed and documented. It includes financial risks but also other risks such as reputational damage.
- 1.4.4 **Due Diligence:** *Knowing exactly who we are dealing with can help to protect our organisation from taking on people who might be less than trustworthy.*
- 1.4.5 **Communication:** *Communicating our policies and procedures to staff and to others who will perform services for us enhances awareness and helps to deter bribery by making clear the basis on which our organisation does business.*
- 1.4.6 **Monitoring and Review:** we monitor and review procedures designed to prevent bribery by persons associated with it and makes improvements where necessary.

- 1.5 Prior to 2011, under Common Law, a person commits an offence where a person *“Offering, giving or receiving, any undue reward, by or to any person whatsoever in a public office, in order to influence his behaviour in office and incline him to act contrary to the known rules of honesty and integrity.”*

Corruption

- 1.6 Corruption can be committed in many ways but normally involves *“two or more people entering into a secret agreement.”*
- 1.7 Indicators showing this type of offending can include the following:
 - 1.7.1 Abnormal cash payments.
 - 1.7.2 Pressure exerted for payments to be made urgently or ahead of schedule.
 - 1.7.3 Private meetings with public contractors or companies hoping to tender for contracts.
 - 1.7.4 Lavish gifts being offered or received.
 - 1.7.5 An individual who never takes time off even if ill, or holidays, or insists on dealing with specific contractors himself or herself.
 - 1.7.6 Making unexpected or illogical decisions accepting projects or contracts.
 - 1.7.7 Abuse of the decision process or delegated powers in specific cases.
 - 1.7.8 Agreeing contracts not favourable to the organisation either because of the terms or the time period.
 - 1.7.9 Unexplained preference for certain contractors during tendering period.
 - 1.7.10 Avoidance of independent checks on the tendering or contracting processes.
 - 1.7.11 The Council’s or its suppliers / partner’s procedures or guidelines not being followed.

- 1.8 The Local Government Act 1972 requires under section 117(2) that employees must disclose any personal interest in contracts that have been, or are proposed to be, entered into by the Council. Failure to do so is a criminal offence.



FRAUD AFFECTS COUNCILS TOO

Have you seen anything suspicious?

- Unusual applications for council services
- Suspicious identity documents or transactions
- Suppliers not delivering what we pay for

If you suspect it, report it.

Call in confidence on **03000 999 111** or
visit **southend.gov.uk/fraud**

This page is intentionally left blank

Counter-Money Laundering Policy and Strategy

VERSION CONTROL SHEET

| | |
|--------------------------|--|
| Title: | Counter-Money Laundering Policy & Strategy |
| Purpose: | To advise council workers and suppliers on what money laundering is, how to identify it and report it. |
| Owner: | Counter Fraud & Investigation Directorate |
| Approved by: | Corporate Management Team – 07/08/2019 Cabinet – 17/09/2019 |
| Date: | Approved – 17/09/2019 Implemented – 18/09/2019 |
| Version Number: | 2.2 |
| Status: | Draft |
| Review Frequency: | Bi-annually |
| Next Review Date: | September 2021 |

| Change History | | |
|----------------|--|---|
| Date | Change Details | Approved by |
| May 2017 | Inclusion of 4 th Money Laundering Directive | Joe Chesterton (Head of Finance & Resources) |
| August 2019 | Revision of formatting and reporting methods, legislative changes. | Joe Chesterton, Executive Director (Finance & Resources) John Williams, Executive Director (Legal & Democratic Services) |

Counter-Money Laundering Policy Statement

Southend-on-Sea Borough Council is serious about protecting public money and ensuring that criminals do not use the council in their enterprises.

Money laundering is a serious crime and recognised as a 'critical enabler' for organised criminal gangs and terrorists to benefit and use for other criminality. Denying criminals the use of their ill-gotten gains disrupts criminality and can help law enforcement identify offenders.

The UK has developed strong legislation to tackle the problem with the right focus being on the financial services industries that are largely targeted to launder the proceeds of crime. The 'regulated sector', as it is known, has experienced and robust processes to make it difficult for criminals to launder their criminal proceeds.

As this work by the banks, financial institutions, legal and property related firms becomes more successful the way criminals launder their illegal money becomes more difficult for them.

The effect of this success is that more and more public bodies are being targeted by criminals to launder their criminal proceeds.

Southend-on-Sea Borough Council takes a strong stance against any criminality. Our dedicated Criminal Finances Unit in the Counter Fraud & Investigation Directorate is experienced in using their powers to identify, seize and confiscate criminal proceeds. We need to ensure that the entire council is live to this reality and works hard to prevent and detect it.

We will continue to work closely with our partners in the National Crime Agency to share information and intelligence and pursue criminals who seek to use the council as a money laundering vehicle.

Ali Griffin

Chief Executive

Contents

| | |
|--|----------|
| 1. Introduction..... | 3 |
| 2. What is Money Laundering?..... | 3 |
| 3. What are the Money Laundering criminal offences? | 4 |
| 4. How to identify suspected Money Laundering | 5 |
| 5. How to report suspected Money Laundering | 5 |
| 6. What does the council do about Money Laundering? | 6 |
| 7. Monitoring Delivery | 6 |
| 8. Relevant Legislation..... | 7 |
| 9. Appendix 1 – Key Contacts | 8 |

1. Introduction

- 1.1 An overriding responsibility of all public sector organisations is the provision of effective and efficient services to our residents in a manner that seeks to ensure the best possible protection of the public funds we use.
- 1.2 This policy sets out the action we will take to mitigate the risk that money could be laundered through our systems.
- 1.3 The legislative requirements concerning anti-money laundering procedures are lengthy and complex. Whilst the risk to the Council of contravening the legislation is relatively low, it is extremely important that all Council and schools workers are familiar with their legal responsibilities. Serious criminal sanctions may be imposed for breaches of the legislation, including imprisonment.
- 1.4 As a responsible public body we expect all of our suppliers and contractors to follow our strong stance and not tolerate any criminality attempting to affect our services or staff.

2. What is Money Laundering?

- 2.1 Money laundering is the process through which 'criminal property' (i.e. a person's benefit from criminal conduct) is given the appearance of having originated from a legitimate source.
- 2.2 Criminal conduct is anything that is a criminal offence in the United Kingdom. It could be fraud, theft, drug dealing, prostitution, terrorism and includes offences such as breaching building planning law and trade mark offences
- 2.3 Criminal property is defined as anything which is a person's benefit from their criminal conduct. That could be money, real and personal property (houses, buildings, boats, cars, horses, watches etc), 'things in action' and other intangible or incorporeal property (i.e. debts, intellectual property such as copyright, designs and patents etc)

3. What are the Money Laundering criminal offences?

Proceeds of Crime Offences

- 3.1 The criminal offences of money laundering are contained in the Proceeds of Crime Act 2002. They are committed when ‘criminal property’ is transferred, concealed, disguised, converted or removed by a person from England, Wales, Scotland & Northern Ireland.
- 3.2 A person also commits the offence of ‘money laundering’ if they enter into or become concerned in an arrangement which they know or suspect facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person
- 3.3 A person commits a criminal offence when they do something that might prejudice ‘a money laundering investigation’, for example, falsifying or concealing a document or ‘tipping off’ (“telling”) a person who is suspected of being involved in money laundering.

Terrorist Financing Offences

- 3.4 The Terrorism Act 2000 also creates money laundering offences where a person enters in to or becomes concerned in an arrangement which facilitates the retention or control by or on behalf of another person of terrorist property (“money”);
- by concealment
 - by removal from the United Kingdom
 - by transfer to nominees, or
 - in any other way
- 3.5 It should be understood that ‘terrorist property’ covers not only the money stolen in, say, a terrorist robbery, but also any money paid in connection with the commission of terrorist acts. Any resources of a proscribed organisation are also covered: not only the resources they use for bomb-making, arms purchase etc but also money they have set aside for non-violent purposes such as paying their rent.
- 3.6 A proscribed organisation is defined under Schedule 2 of the Terrorism Act 2000. The Counter Fraud & Investigation Directorate is responsible for monitoring these organisations and responding appropriately.

- 3.7 A person also commits a criminal offence if they fail to disclose to a constable that they believe a person has committed a terrorism money laundering offence.

Criminal Law Defences

- 3.8 A person does not commit a criminal offence where they can demonstrate that ***“his employer has established a procedure for the making of disclosures of the matters specified”*** and they follow that procedure.

4. How to identify suspected Money Laundering

- 4.1 All council workers should be alert to the possibility of someone trying to launder criminal proceeds through the Council. Some indications of suspicious activity are:

- △ Large cash payments (e.g. paying business rates in cash)
- △ Overpayments by a person/ company in any way
- △ Duplicate payments by a person/ company in any way
- △ Regular requests for refunds of payments
- △ Regular ‘chargebacks’ for card payments
- △ Someone paying on behalf of a third party
- △ Cash buyers purchasing land or property (e.g. Right to Buy properties)

- 4.2 Any council workers with concerns about money laundering should contact a member of the Counter Fraud & Investigation Directorate (CFID) on **03000 999111** for advice.
- 4.3 CFID regularly provides training to council services on identifying and reporting suspected money laundering.

5. How to report suspected Money Laundering

- 5.1 The Counter Fraud & Investigation Directorate (CFID) is responsible for managing any cases of suspected money laundering.
- 5.2 It is the responsibility of every council worker to look for and report any possible money laundering taking place. You **do not** have to speak to a manager before reporting your suspicions.
- 5.3 If you see any of the suspicious activity linked to money laundering **you should**:
- △ Not tell the person that you have any suspicions about them
 - △ Take all the records (and any cash) from the person to a secure location
 - △ Telephone a member of the CFID team right away on **03000 999111 (24/7)**
 - △ Follow the instructions given by the CFID team.
- 5.4 **Remember:** Failure to report your suspicions to CFID could expose *you* to criminal prosecution.

6. What does the council do about Money Laundering?

- 6.1 The Criminal Finances Unit in the Counter Fraud & Investigation Directorate is accredited by the National Crime Agency to conduct money laundering investigations. The Accredited Financial Investigators in the team can obtain court Production Orders to access a person's bank accounts, seize any cash and restrain a person's assets, worldwide, who they suspect of money laundering.
- 6.2 In cases where money laundering is proven the council will prosecute those offenders and use the Proceeds of Crime Act 2002 to take their ill-gotten gains. Any money confiscated is paid back in to the council to fight crime.

7. Monitoring Delivery

- 7.1 The Counter Fraud & Investigation Directorate leads the council's fight against fraud and economic crime, including money laundering. The team reports quarterly to the Council's Audit Committee on its work to tackle the problem.
- 7.2 The service also reports regularly on its performance to the Council's Corporate Management Team.

8. Relevant Legislation

- 8.1 The Terrorism Act 2000 as amended by the Anti-Terrorist Crime and Security Act 2001
- 8.2 The Proceeds of Crime Act 2002 (POCA)
- 8.3 Serious Organised Crime and Police Act 2005
- 8.4 The Money Laundering Regulations 2007
- 8.5 Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (*known as the EU 4th Money Laundering Directive*)

9. Appendix 1 – Key Contacts

| Contact | Details |
|---|---|
| Counter Fraud & Investigation Directorate | 9 th Floor, Civic Centre, Victoria Avenue, Southend-on-Sea, SS2 6EN Tel: 03000 999 111 E-mail: counterfraud@southend.gov.uk Web: southend.gov.uk/fraud |
| David Kleinberg Assistant Director for Fraud & Investigation | Tel: 03000 999 111 E-mail: davidkleinberg@southend.gov.uk |
| Joe Chesterton Strategic Director (Finance & Resources) <i>(s.151 Chief Finance Officer)</i> | 10 th Floor, Civic Centre, Victoria Avenue, Southend-on-Sea, SS2 6EN Tel: 01702 215200 E-mail: joechesterton@southend.gov.uk |
| John Williams Strategic Director (Legal and Democratic Services) <i>(Monitoring Officer)</i> | 2 nd Floor, Civic Centre, Victoria Avenue, Southend-on-Sea, SS2 6EN Tel: 01702 215102 E-mail: johnwilliams@southend.gov.uk |
| Andrew Barnes Head of Internal Audit | 9 th Floor, Civic Centre, Victoria Avenue, Southend-on-Sea, SS2 6EN Tel: 07827 348375 E-mail: andrewbarnes@southend.gov.uk |
| Protect <i>(Independent charity for whistleblowing, providing free independent legal advice)</i>  | CAN Mezzanine, 7-14 Great Dover Street, London SE1 4YR Tel: 020 3117 2520 E-mail: whistle@protect-advice.org.uk Web: pcaw.org.uk |



MONEY LAUNDERING

Could you spot the signs?

- Cash payments over £1,500
- A person regularly receiving account refunds
- One person paying the debts for several individuals

If you suspect it, report it.

Call in confidence on **03000 999 111** or
visit **southend.gov.uk/fraud**

This page is intentionally left blank



WHISTLEBLOWING "CONFIDENTIAL REPORTING" POLICY AND PROCEDURE

PRODUCED BY: HEAD OF INTERNAL AUDIT

SUBJECT TO BI ANNUAL REVIEW

PRESENTED TO:

CORPORATE MANAGEMENT TEAM: AUGUST 2019

CABINET: SEPTEMBER 2019

AUDIT COMMITTEE: OCTOBER 2019

WHISTLEBLOWING POLICY

VERSION CONTROL SHEET

| | |
|--------------------------|--|
| Title: | Whistleblowing Policy |
| Purpose: | The policy and procedure have been developed so that council workers will know how to raise concerns in the right way at an early stage, and to enable managers to understand their responsibilities in relation to allegations of misconduct and impropriety. |
| Owner: | Monitoring Officer |
| Approved by: | Corporate Management Team – 07/08/2019 Cabinet – 17/09/2019 |
| Date: | Approved – 17/09/2019 Implemented – 18/09/2019 |
| Version Number: | 2.1 |
| Status: | Draft |
| Review Frequency: | Bi-annually, subject to legislative changes and operational changes |
| Next Review Date: | September 2021 |

| Change History | | |
|----------------|--|---|
| Date | Change Details | Approved by |
| March 2013 | Revision of formatting and reporting methods, legislative changes. | Joe Chesterton, Head of Finance & Resources |
| August 2019 | Revision of formatting, reporting details and officer details. | Joe Chesterton, Executive Director (Finance & Resources) John Williams, Executive Director (Legal & Democratic Services) |

WHISTLEBLOWING POLICY

INTRODUCTION

The council is committed to providing the highest quality service to those that live, work, visit, do business and study in the borough. This involves ensuring that the local community can have full trust and confidence in the way the Council manages its services and resources and making sure that all those who are vulnerable such as children, the elderly and people with learning disabilities are provided for safely, effectively and in accordance with best practice.

Employees, workers or contractors at one time or another may have concerns about what is happening at their work with Southend-on-Sea Borough Council ("the Council"). Usually these concerns are easily resolved by speaking to their manager without using a formal process. The Council has this Whistleblowing Policy and Procedure to enable employees, workers or contractors to raise more serious concerns.

This Whistleblowing Policy cannot be used by employees who have a grievance regarding their own employment, who should use the Grievance processes, or by members of the public, who should use the Council's Complaints processes.

The Council is committed to the highest standards of openness, probity and accountability. In line with that commitment we encourage employees, workers and contractors with serious concerns about any aspect of the Council's work to come forward and voice their concerns. The Council would rather they raised the matter when it is just a concern rather than wait for proof. It is recognised that certain cases will have to proceed on a confidential basis. This Whistleblowing Policy makes it clear that such concerns can be raised without fear of reprisals.

This Whistleblowing Policy is not intended for initial reporting of minor lapses of standards, inaction or incidents. If, however, employees, workers or contractors have something more serious that is troubling them which they have discussed with their manager but feel that they have not been taken seriously, or due to the sensitivity of the matter feel they cannot raise their concerns within their service, then they should use this Whistleblowing Policy.

LEGISLATIVE BACKGROUND

The Public Interest Disclosure Act 1998 protects workers making disclosures about certain matters of concern, where those disclosures are made in accordance with the Act's provisions.

The 1998 Act is incorporated into the Employment Rights Act 1996, which also protects employees who take action over, or raise concerns about health and safety at work.

WHISTLEBLOWING POLICY

DEFINITION

Any serious concerns that employees, workers or contractors have about any aspect of service provision or the conduct of Councillors, officers of the Council or others acting on behalf of the Council can be reported under the Whistleblowing Policy.

Workers are protected by law (under the Public Interest Disclosure Act 1998) from any possible reprisals or victimisation for having raised any issues where they **reasonably believe** that in appropriate actions are being, or will be, undertaken. These may include:

- a criminal offence
- fraud & corruption, including bribery
- failure to comply with legislation
- failure to comply with good practice, especially where this endangers children and/or vulnerable adults
- disclosure relating to miscarriage of justice
- health and safety risks, including risks to the public as well as other employees
- damage or danger to the environment
- sexual, physical, emotional or psychological abuse of clients
- failure to comply with the Employees or Members Code of Conduct
- theft of Council property and assets
- failure to comply with the Council's rules on gifts and hospitality
- serious mismanagement or failure to manage
- continuing inappropriate conduct or behaviour or performance by any employee which has been reported to a relevant manager, especially harassment or bullying or discriminatory behaviour. This may include, but not be confined to, actions considered to be based upon the race, gender, disability, age, religion/belief or sexual orientation of the victim
- a cover up of, or failure to report, any of the above.

Under the Public Information Disclosure Act 1998 a "protected disclosure" is specified under section 43B. Not all disclosures detailed in this paragraph offer 'protected disclosure' under the Act. However the Council undertakes to extend the same protection for all disclosures wherever possible.

COMMITMENT OF THE COUNCIL

The Council is committed to considering the concerns of employees, workers or contractors and will take actions as appropriate in line with the Whistleblowing Procedure outlined in this policy.

WHISTLEBLOWING POLICY

SAFEGUARDS

Harassment or victimisation

The Council recognises that the decision to report a concern can be a difficult one to make, not least because of the fear of reprisal from those responsible for the malpractice. The Council will not tolerate harassment or victimisation and will take action to protect employees, workers or contractors when they raise a concern in good faith.

The Council will treat any harassment or victimisation as a serious disciplinary offence to be dealt with under the Discipline and Dismissal at Work Policy.

This does not mean that if employees are already the subject of disciplinary, redundancy or other procedures that those procedures will be halted as a result of their whistleblowing.

Confidentiality

The Council recognises that employees, workers or contractors may nonetheless want to raise a concern in confidence under this Whistleblowing Policy. If an employee, worker or contractor asks the Council to protect their identity, the Council will do its best not to disclose it without their consent. If the situation arises where the Council is not able to resolve the concern without revealing the employee, worker or contractors identity (for instance because their evidence is needed in court), we will discuss with them whether and how we can proceed.

Anonymous allegations

This Whistleblowing Policy encourages employees, workers or contractors to put their name to their allegation. Concerns raised anonymously are much less powerful but they will be considered at the discretion of the Council.

In exercising the discretion the factors to be taken into account would include:

- the seriousness of the issues raised
- the credibility of the concern
- the likelihood of confirming the allegation.

Untrue allegations

If an employee makes an allegation in good faith but it is not confirmed by the investigation no action will be taken against them. If however, an employee makes a malicious or vexatious allegation, disciplinary action may be taken against them.

THE MONITORING OFFICER (EXECUTIVE DIRECTOR (LEGAL AND DEMOCRATIC SERVICES))

The Executive Director (Legal and Democratic Services) is the Monitoring Officer for the Council. The Monitoring Officer has overall responsibility for the maintenance and operation of this Whistleblowing Policy and Procedure.

WHISTLEBLOWING POLICY

The Counter Fraud & Investigation Directorate maintains a record of concerns raised under the Whistleblowing Policy and Procedure and the outcomes of any investigation undertaken on behalf of the Monitoring Officer, who will report if necessary to the Standards Committee. This is done in a form that does not endanger employee, worker or contractor confidentiality.

The Monitoring Officer will consult with such other Council officers as he or she considers necessary and may arrange for any investigation to be conducted and dealt with in such manner as he or she decides.

SCOPE OF POLICY

- This Whistleblowing Policy applies to all employees, workers and contractors working for the Council, for example agency workers, builders, drivers etc. to enable them to raise serious concerns that they have about any aspect of service provision or the conduct of Councillors, officers of the Council or others acting on behalf of the Council
- This Whistleblowing Policy cannot be used by employees who have a grievance regarding their own employment, who should use the Grievance processes, or by members of the public, who should use the Council's Complaints processes.

DELEGATION

- All managers are authorised to discuss and act upon employees concerns about what is happening at work without using the formal process of the Whistleblowing Policy
- The Monitoring Officer (Executive Director (Legal & Democratic Services)), Corporate Directors, Heads of Service and the Head of Internal Audit are authorised to act (in conjunction with the Counter Fraud & Investigation Directorate) upon serious concerns raised under the Whistleblowing Policy, in accordance with the Whistleblowing Policy and Procedure
- All concerns raised under this Whistleblowing Policy will be notified to the Counter Fraud & investigation Directorate
- All concerns raised under this Whistleblowing Policy regarding financial issues will also be notified to the Head of Internal Audit.

WHISTLEBLOWING POLICY

WHISTLEBLOWING PROCEDURE

HOW TO RAISE A CONCERN

Employees who raise concerns that fall within the scope of other Council Procedures will not be dealt with under this Whistleblowing Procedure, but will be advised on the appropriate procedure to use. Such employees will still receive protection as detailed in the Whistleblowing Policy.

Employees, workers or contractors should normally raise concerns with their immediate manager, without needing to use the Whistleblowing Policy. This depends, however, on the seriousness and sensitivity of the issues involved and who is thought to be involved in the malpractice.

Where a concern is serious or where it is a concern about the line manager, or having made a report they believe that their manager has failed to take appropriate action, the employee, worker or contractor should contact:

- the Counter Fraud & Investigation Directorate on 03000 999111 or via counterfraud@southend.gov.uk or
- the Council's Confidential Report Line on 01702 215215

Concerns should be raised in writing, clearly marked “**Whistleblowing, Counter Fraud & Investigation Directorate**” and placed in an envelope marked “**Staff in Confidence**”. The background and history of the concern (giving names, dates, and place where possible), and the reasons for the concern should be set out.

The earlier employees, workers or contractors express a concern, the easier it is to take action. Employees may invite a trade union representative or work colleague to raise a matter on their behalf.

All concerns raised under this Whistleblowing Policy regarding financial issues will also be notified to the Head of Internal Audit.

HOW THE COUNCIL WILL RESPOND

Once an employee, worker or contractor has raised their concern under the Whistleblowing Policy with the Counter Fraud & Investigation Directorate, initial enquiries will be made to decide if an investigation is appropriate and if so what form the investigation should take.

The employee, worker or contractor will be advised of the following:

- who is considering the issue
- how that person can be contacted
- whether their further assistance may be needed.

The senior officer responsible for considering the issue will write to the employee, worker or contractor summarising their concern and setting out how the Council proposes to handle it, if requested to do so. The employee, worker or contractor will also be requested to state any personal interest they may have in the matter.

WHISTLEBLOWING POLICY

The overriding principle which the Council will have in mind is the public interest. Concerns or allegations which fall within the scope of specific procedures (for example, child protection or discrimination issues) will normally be referred for consideration under those procedures. The action taken by the Council will depend on the nature of the concern and may:

- be resolved by agreed action without the need for investigation
- be investigated internally
- be referred to the police
- be referred to the external auditor
- form the subject of an independent inquiry.

The amount of contact between the employee, worker or contractor and the officers investigating the concerns will depend on the concerns raised, but the Council may need to seek further information from the employee, worker or contractor. Any meetings may be arranged on or off site and an employee may be accompanied by a friend, union or professional body representative.

While the purpose of this Whistleblowing Policy is to enable the Council to investigate possible malpractice and take appropriate steps to deal with it, they will provide as much feedback to the employee, worker or contractor as they properly can. If requested, confirmation of the response may be provided in writing. It may not, however, be possible to advise the precise action that will be taken where this would infringe a duty of confidence owed by the Council to someone else.

HOW A CONCERN CAN BE TAKEN FURTHER

If you are unsure whether or how to use this procedure or want independent advice, you may contact the independent charity, **Protect** (formerly known as Public Concern at Work) on 020 3117 2520. Their lawyers can give you free confidential advice at any stage on how to raise a concern about serious malpractice at work.

The Whistleblowing Policy is intended to provide employees, workers or contractors with the reassurance they may need to raise concerns internally and that they will be satisfied with any action taken.

However, if they are not, and feel that it is appropriate to take the matter outside the Council or if they feel unable to raise their concerns internally, the Council would rather they raised the matter with an appropriate regulator than not at all. The following are possible contact points:

- Local Council Member
- Local Government Ombudsman
- The employee's trade union
- Local Citizens Advice Bureau
- The Police
- Relevant professional bodies, regulatory or other organisations.

If employees, workers or contractors take their concerns outside the Council they should take care not to disclose any confidential information.



**Policy and Procedures
for undertaking Directed Covert Surveillance
and the use of Covert Human Intelligence Sources**

Produced by

- Internal Audit Services, April 2010
- Updated w 1st November 2012
- Updated May 2014
- Updated June 2016
- UPDATED OCTOBER 2016
- UPDATED SEPT 2018
- UPDATED SEPT 2019

CONTENTS

PART 1

POLICY FOR UNDERTAKING DIRECTED COVERT SURVEILLANCE AND USE OF COVERT HUMAN INTELLIGENCE SOURCES

| | Pages |
|---|-------|
| 1 Introduction | 4-5 |
| 2. Background | 6-7 |
| 3 What is Surveillance? | 7-10 |
| 4 What is a Covert Human Intelligence Source (CHIS)? | 10-11 |
| 5 Procedural principles for Surveillance and use of CHISs | 11-14 |
| 6. Surveillance outside of RIPA | 14-16 |
| 7. Internet and Social Media - use for Research and Investigations | 16-17 |
| 8 Use of CCTV | 17 |
| 9 Use of material as evidence | 17-18 |
| 10. Safeguards of material | 18 |
| 11. Errors | 18-19 |
| 12. Complaints | 19-20 |
| 13 Oversight by Investigatory Powers Commissioner | 20-21 |

PART 2

DETAILED PROCEDURES FOR UNDERTAKING DIRECTED COVERT SURVEILLANCE

| | | |
|----|---------------------------|-------|
| 1. | Purpose | 22 |
| 2 | Scope | 22 |
| 3 | Procedure | 22-28 |
| 4 | Joint Agency Surveillance | 28 |

PART 3

DETAILED PROCEDURES FOR USE OF COVERT HUMAN INTELLIGENCE SOURCES

29

| | |
|-------------------|--|
| APPENDIX 1 | <i>a) Flow Chart Directed Surveillance</i> |
| | <i>b) Sample application form for use of Directed Covert Surveillance</i> |
| APPENDIX 2 | <i>a) Flow Chart for the procedure for the Application to the Justice of the Peace for an order to approve the grant of a RIPA Authorisation or Notice</i> |
| | <i>b) Copy application form and order for judicial approval</i> |
| APPENDIX 3 | <i>Internet Guidance – a summary of the Covert Surveillance and Property Interference Revised Code of Practice 2018.</i> |

PART 1

POLICY FOR UNDERTAKING DIRECTED COVERT SURVEILLANCE AND USE OF COVERT HUMAN INTELLIGENCE SOURCES

1. Introduction

1.1 The performance of certain investigatory functions of Local Authorities may require the surveillance of individuals or the use of informants. Such actions may intrude on the privacy of individuals and can result in private information being obtained and as such, should not be undertaken without full and proper consideration. Legislation now governs how Local Authorities should administer and record surveillance and the use of informants and renders evidence obtained lawful for all purposes. This Policy sets out the Council's rules and procedures.

1.2 The purpose of this Policy is to ensure there is a consistent approach to the undertaking and authorisation of surveillance activity. Therefore, this Policy is to be used by all Council service areas and officers undertaking investigation work and using the techniques of surveillance or the use of Covert Human Intelligence Sources (CHIS's).

1.3 In this Policy the following terms shall have the meanings stated:

"Investigating Officer" – shall mean any Council officer undertaking or wishing to undertake directed covert surveillance or to use a CHIS provided he / she has received appropriate training.

"Authorising Officer" – shall mean.

- i) All Chief Officers who have received appropriate training
- ii) Holders of the following three posts provided he/she has received appropriate training – Group Manager for Environmental Health, Group Manager Waste and Environmental Care and the Director for Public Protection

"Senior Responsible Officer" – shall mean the Executive Director (Legal & Democratic Services) John Williams
johnwilliams@southend.gov.uk

"Principal Legal Executive" – shall mean the officer with this job title currently Tessa O'Connell
tessaoconnell@southend.gov.uk

- 1 4 This Policy was updated in November 2012 to reflect the provisions of the Protection of Freedoms Act 2012 which from the 1st November 2012 requires that a Justice of the Peace ("JP") must approve all Local Authority RIPA applications and renewals

Two guidance documents explaining this authorisation process have been issued by the Home Office to Local Authorities and Magistrates and these are available on the following links

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/118173/local-authority-england-wales.pdf

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/118174/magistrates-courts-eng-wales.pdf

This Policy was updated in June 2016 to incorporate additional information on surveillance outside RIPA in Section 6 and regarding the internet and social media for research and investigations in Section 7

This Policy was updated in September 2018 to reflect the "Covert Surveillance and Property Interference Revised Code of Practice" issued by the Home Office ("the 2018 Code") and this can be accessed using the link below

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742041/201800802_CSPI_code.pdf

- 1 5 RIPA was overseen by the Office of Surveillance Commissioners (OSC) However, from 1 Sept 2017 oversight transferred to the Investigatory Powers Commissioner's Office (IPCO) IPCO is the independent inspection regime whose remit includes providing comprehensive oversight of the use of the powers to which the 2018 Code applies, and adherence to the practices and processes described in it IPCO also provides guidance to be followed which is separate from the 2018 Codes

- 1.6 This Policy is intended to be a best practice guide It is not intended to replace the 2018 Code and where necessary the Code should be consulted. However, following this Policy ensures compliance with the 2018 Codes

- 1 7 This Policy is not intended to be an exhaustive guide and specific legal advice should be sought if Council officers do not find questions answered after reading this document and the 2018 Code. Officers should always consult the Legal Team before seeking authorisation

2. Background

- 2.1 On 2nd October 2000 the Human Rights Act 1998 (HRA) came into force making it potentially unlawful for a Local Authority to breach any article of the European Convention on Human Rights (ECHR). Any such breach may now be dealt with by the UK courts directly, rather than through the European Court at Strasbourg.
- 2.2 Article 8 of the ECHR states that everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of
- National security
 - Public safety
 - The economic well-being of the country
 - The prevention of disorder or crime
 - The protection of health or morals
 - The protection of the rights and freedoms of others
- 2.3 The performance of certain functions by Local Authorities may require the directed covert surveillance of individuals or the use of informants or undercover officers, known as CHIS.
- 2.4 Those who undertake directed covert surveillance on behalf of a Local Authority may breach an individual's human rights, unless such surveillance is consistent with Article 8 of the ECHR and is both necessary and proportionate to the matter being investigated.
- 2.5 As a result of the legislative changes referred to in 1 above, Local Authorities can now only authorise directed covert surveillance under RIPA for the purpose of preventing or detecting conduct which constitutes a **criminal offence** which is:
- (a) punishable (whether on summary conviction or indictment) by a maximum term of at least six months imprisonment; or
 - (b) involves the sale of alcohol or tobacco to children
- 2.6 Furthermore, if authorised by an authorised officer, the Council's authorisation can only be given effect once an Order approving the authorisation has been granted by a JP.

It is important to note

- A Local Authority cannot authorise the use of directed covert surveillance under RIPA to investigate low level offences e.g. littering, dog control and fly posting. Neither can a Local Authority authorise such surveillance for the purpose of preventing disorder, unless this involves a criminal offence punishable in the way described above.
- The crime threshold referred to above applies only to the authorisation of directed covert surveillance under RIPA, not to the authorisation of Local Authority use of CHIS or their acquisition of communications data.

- 2.7 In order to properly regulate the use of directed covert surveillance and the use of CHISs in compliance with the HRA, the Regulation of Investigatory Powers Act 2000 (RIPA) came into force on 25th September 2000.
- 2.8 RIPA requires that all applications to undertake directed covert surveillance of individuals or to use CHISs are properly authorised, recorded and monitored. The detailed procedure for undertaking directed covert surveillance or using a CHIS are set out in Parts 2 and 3.
- 2.9 Failure to comply with RIPA may leave the Council open to potential claims for damages or infringement of individual's human rights. It may also mean that any evidence obtained in breach of the provisions of RIPA is rendered inadmissible in Court.

3. What is Surveillance?

3.1 Surveillance is

- Monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications.
- Recording anything monitored, observed or listened to in the course of surveillance, with or without the assistance of a device.

- 3.2 By its very nature, surveillance involves invading an individual's right to privacy. The level of privacy which individuals can expect depends upon the nature of the environment they are within at the time. For example, within an individual's own home or private vehicle, an individual can expect the highest level of privacy. The level of expectation of privacy may reduce if the individual transfers out into public areas.

- 3.3 There are different types of surveillance which, depending on their nature, are either allowable or not allowable and require different degrees of authorisation and monitoring under RIPA.

3.4 **Overt surveillance** is where the subject of surveillance is aware that it is taking place. Overt surveillance is outside the scope of RIPA and therefore does not require authorisation. The 2018 Code also provides guidance that authorisation under RIPA is not required for the following types of activity:

- General observations that do not involve the systematic surveillance of an individual or a group of people
- Use of overt CCTV surveillance
- Surveillance where no private information is likely to be obtained
- Use of overt ANPR systems to monitor traffic flows or detect motoring offences
- Surveillance undertaken as an immediate response to a situation
- Review of staff usage of the internet & e-mail (but see Section 6.7 below)
- Surveillance not on statutory grounds (see section 6 Surveillance outside of RIPA)

3.5 **Covert surveillance** is defined as “surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place” and is covered by RIPA. Covert surveillance is categorised as either intrusive or directed.

3.6 **Intrusive covert surveillance** is defined as covert surveillance that is carried out in relation to anything taking place on any residential premises or in any private vehicle and involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device. RIPA does not empower Local Authorities to authorise or undertake intrusive covert surveillance. Other means of investigation should be considered.

3.7 **Directed covert surveillance** is surveillance which is covert but not intrusive and undertaken.

- For the purposes of a planned specific investigation or operation,
- In such a manner as is likely to result in the obtaining of private information about a person (whether or not that person is specifically targeted for the purposes of an investigation or operation), and
- Other than by immediate response to circumstances when it would not be practical to seek authorisation, for example, noticing suspicious behaviour and continuing to observe it.

3.7.1 **Private information** includes any information relating to a person’s private or family life. As a result, private information is capable of including any aspect of

a person's private or personal relationship with others, such as family and professional or business relationships

Note: Information which is non-private includes

- Publicly available information such as books, newspapers, journals, TV and radio broadcasts, newswires, web sites, mapping imagery, academic articles, conference proceedings, business reports, and more.
- Commercially available data where a fee may be charged, and any data which is available on request or made available at a meeting to a member of the public

3 7 2 Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by a public authority of that person's activities for future consideration or analysis. Surveillance of publicly accessible areas of the internet should be treated in a similar way, recognising that there may be an expectation of privacy over information which is on the internet, particularly where accessing information on social media websites (see 7 below)

3.7 3 Private information may include personal data, such as names, telephone numbers and address details. Where such information is acquired by means of directed covert surveillance of a person having a reasonable expectation of privacy, authorisation is required

3.7 4 Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish, for example, a pattern of behaviour, or if one or more pieces of information (whether or not available in the public domain) are covertly (or in some cases overtly) obtained for the purpose of making a permanent record about a person or for subsequent data processing to generate further information. In such circumstances, the totality of information gleaned may constitute private information even if individual records do not. Where such conduct includes covert surveillance, a directed surveillance authorisation may be considered appropriate

3 7 5 Directed covert surveillance involves the observation of a person or persons with the intention of gathering private information to produce a detailed picture of a person's life, activities and associations

3 7 6 Directed covert surveillance does not include entry on or interference with property or wireless telegraphy but may include the use of photographic and video equipment (including the use of CCTV)

3 7 7 Directed covert surveillance is covered by RIPA and requires prior authorisation

4. What is a Covert Human Intelligence Source (CHIS)?

4 1 A CHIS is defined in section 25(7) of the RIPA as a person who establishes or maintains a personal or other relationship with another person for the covert purpose of facilitating anything that

(a) Covertly uses such a relationship to obtain information or to provide access to any information to another person, or

b) Covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship

4 2 By virtue of section 26(9)(b) of RIPA a purpose is covert, in relation to the establishment or maintenance of a personal or other relationship, if and only if, the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose

4 3 By virtue of section 26(9)(c) of RIPA a relationship is used covertly, and information obtained as above is disclosed covertly, if and only if it is used or, as the case may be, disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.

4 4 Special consideration must be given to the use of Vulnerable Individuals as a CHIS. A 'Vulnerable Individual' is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself, or unable to protect himself against significant harm or exploitation. Any individual of this description, or a Juvenile as defined below, should only be authorised to act as a source in the most exceptional circumstances and only then when authorised by the Chief Executive (or, in her absence, the Deputy Chief Executive).

4.5 Special safeguards also apply to the use or conduct of Juvenile Sources; that is sources under the age of 18 years. On no occasion should the use or conduct of a source under 16 years of age be authorised to give information against his parents or any person who has parental responsibility for him

4.6 Legal advice must be sought if considering using a vulnerable or juvenile CHIS.

4 7 It is not anticipated that CHISs will be used often in the normal course of Council investigatory activity. Any Council Officer considering the use of a

CHIS must first contact the Senior Responsible Officer or the Principal Legal Executive to discuss the suitability of this approach

4 8 Authorisation is not required when individuals, including members of the public, are requested to provide information pertaining to other individuals, unless they are required to form a relationship, or manipulate an existing relationship with those other individuals

4 9 Detailed procedures for the use of CHIS are set out in Part 3.

5. Procedural principles for Surveillance and use of CHIS's

5 1 Detailed procedures for undertaking directed covert surveillance are set out in Parts 2 and 3 of this Policy respectively

5 2 The conduct of surveillance which is consistent with these procedures can be undertaken with confidence that any evidence obtained will be admissible in a criminal trial, provided the conduct is authorised and is carried out in accordance with the authorisation. The authorisation must be shown to be necessary on the grounds of preventing or detecting crime (see 2.5 above).

5 3 The Investigating Officer seeking authorisation for directed covert surveillance or CHIS activity and the Authorising Officer must give consideration to the following factors

- **Necessity** – Is directed covert surveillance or CHIS activity the only or best way to obtain the desired information in connection with a potential criminal offence of the types referred to in 2 5, or are other less invasive methods appropriate?
- **Proportionality** – Is the surveillance activity or CHIS activity proportional to the evidence that will be obtained and to the privacy the subject could reasonably expect? The methods used to obtain evidence should not be excessive and should be as non-invasive as it possible. The surveillance should not restrict an individual's right for privacy more than is absolutely necessary
- **Collateral Intrusion** – Will the surveillance result in the observing of innocent people? If so can it be avoided or minimised?

5 4 Further Considerations

- Does the application relate to a criminal offence which has a maximum sentence of at least 6 months or relate to the sale of alcohol or tobacco to children
- Have other ways of getting the information been investigated?

- Is surveillance a reasonable approach and “not a sledge hammer to crack a nut”?
 - The risk of the directed surveillance and CHIS activity must be considered and managed
 - Surveillance authorisations remain valid for 3 months but must be cancelled prior to that if no longer required
 - CHIS authorisations remain valid for 12 months and must be cancelled prior to that if no longer required
 - Authorisations should be periodically reviewed by the Authorising Officer and the need for continued surveillance or CHIS activity ascertained; if no longer required, authorisations should be cancelled
- 5.5 All Council officers undertaking directed cover surveillance or wishing to use a CHIS must have received appropriate training to enable them to undertake this task
- 5.6 Training should be periodically arranged to ensure that sufficient Authorising Officers are available
- 5.7 Where directed covert surveillance or the use of a CHIS is likely to result in the obtaining of confidential information, it is imperative that legal advice should first be sought from the Senior Responsible Officer or the Principal Legal Executive. “Confidential information” includes, though is not limited to, matters subject to legal privilege, confidential personal information and confidential journalistic material. Confidential personal information is information held in confidence relating to the physical or mental health or spiritual counselling concerning an individual (whether living or dead) who can be identified from it
- 5.8 The application for authorisation must include the following elements and the Authorising Officer must consider these, before authorising the directed covert surveillance or CHIS activity.
- full details of the reason for the directed covert surveillance or CHIS activity and the intended outcome,
 - the proposed surveillance activity described as fully as possible, with the use of maps or other plans as appropriate,
 - the necessity and proportionality to the potential offence consideration and whether other methods of less intrusive investigation should / have been attempted and whether they are appropriate,
 - the resources to be applied and tactics and methods should also be included,

- the anticipated start date and duration of the activity, if necessary broken down over stages;
 - details (including unique reference number) of any surveillance previously conducted on the individual
- 5 9 In addition the Authorising Officer should notify the Chief Executive of an authorisation
- 5 10 Services that undertake surveillance activity or use of CHISs should put in place adequate arrangements for the retention of evidence gathered. The arrangements must comply with the Criminal Procedure and Investigations Act 1996 and any other relevant guidance or procedures to ensure the integrity of the evidence
- 5.11 Evidence or intelligence obtained as a result of a RIPA authorisation should not be passed to other agencies such as the Police unless the request meets the Data Protection Act 2018 (“DPA”) requirements under the Law Enforcement processing procedures or Schedule 2, Part 1 Paragraph 2 the replacement for section 29 DPA This will assist with oversight of the process
- 5 12 The Authorising Officer's statement on the authorisation form should clearly demonstrate agreement that the activity is necessary and proportionate and that he / she has thoroughly considered the matter before authorising and state exactly what activity is authorised, against whom, where and in what circumstances
- 5 13 The responsibilities of the Senior Responsible Officer are
- Maintaining the Council's RIPA Policy and Procedures
 - Ensuring the integrity of the processes in place within the Council to authorise directed covert surveillance
 - compliance with the legislation and Codes of Practice
 - engagement with the IPCO and inspectors when they conduct their inspections,
 - where necessary, overseeing the implementation of any post inspection action plans recommended or approved by the IPCO, and
 - for ensuring that all *Authorising Officers* are of an appropriate standard in light of any recommendations in the inspection reports prepared by the IPCO. Where an inspection report highlights concerns about the standards of *Authorising Officers*, this individual will be responsible for ensuring the concerns are addressed

- 5.14 The Principal Legal Executive will maintain a Central Record of RIPA Applications and Authorisations (including the JP approval form) This Central Record will be used to track the progress of authorisations and ensure that reviews, renewals and cancellations take place within the prescribed timeframe. Copies of all RIPA authorisations, reviews, renewals and cancellations should be forwarded to the Principal Legal Executive promptly The record will be available to the IPCO, at any time The Central Register format will be consistent with that detailed in the 2018 Code
- 5.15 A report on the use of RIPA will be submitted annually to the Cabinet Cabinet will consider this Policy and review the Council's use of RIPA
- 5.16 The head of each section which undertakes directed surveillance or CHIS activity will ensure that.
- staff receive the necessary training,
 - all activity is in accordance with RIPA and the 2018 Code, and
 - relevant procedures are maintained to ensure the above

6. Surveillance outside of RIPA

- 6.1 As a result of the change in the law from the 1st November 2012 directed covert surveillance under RIPA will only apply to the detection and prevention of a criminal offence that attracts a penalty of 6 months imprisonment or more or relates to the sale of alcohol or tobacco to children This essentially excludes surveillance of many offences that the Council may investigate such as disorder (unless it has 6 months custodial sentence) and most summary offences such as littering, dog fouling etc Other examples are referred to in 6.4 below
- 6.2 This change does not mean that Council enforcement officers cannot undertake such surveillance, but because it is **not** regulated by the IPCO, responsibility for monitoring this type of activity falls to the Council's Senior Responsible Officer (SRO) As a result procedures need to be in place to ensure that the Council can prove that it has given due consideration to necessity and proportionality which are central tenets of European Law and the likely grounds of any challenge
- 6.3 If it is necessary for the Council to undertake surveillance which does not meet the criteria to use the RIPA legislation, (such as in cases of disciplinary investigations against staff or surveillance relating to Anti-Social Behaviour appertaining to disorder) the Council must still meet its obligations under the Human Rights Act and be able to demonstrate that its actions (which may infringe a person's Article 8 rights to privacy) are necessary and proportionate, which includes taking account of the intrusion issues. To demonstrate this accountability, the decision making process and the

management of such surveillance must be documented. Therefore, should Council officers need to undertake such surveillance outside of RIPA, they should complete the Non RIPA Surveillance form (available from the RIPA pages on the intranet). This should be submitted to one of the Authorising Officers listed within this Policy to be considered for authorisation before any activity can be undertaken. There will be no requirement to have the authorisation approved by a Justice of the Peace. Should the activity be approved, the procedures to be followed will be the same as any RIPA authorised activity. Therefore, the Council expects that the procedure and management of the activity, from the initial surveillance assessment, through to completion and cancellation to be managed appropriately at the same level that the RIPA legislation and guidance requires. For further advice, refer to the RIPA pages on the Intranet.

6.4 Examples of Surveillance outside of RIPA

6.4.1 Planning

Some planning scenarios require evidence to be gathered either before service of a Notice or post service of a Notice to establish whether the Notice has been breached. A common example may be someone running a car repair business from home. It is often the case that this causes disruption and disturbance to neighbours who complain. Diary sheets may be issued to establish the level of activity and the person may be spoken to by a Planning Enforcement officer. It is often the case that the person states they only repair a few cars as a hobby for friends and family and are not running a business. At some stage it may be necessary for a Notice to be issued to the person. The repairs may then continue with the neighbours complaining. It is at this stage that targeted covert surveillance may be required as the best means of gathering the required information to establish if the Notice has been breached which would be a criminal offence. The offence does not meet the 6 months imprisonment criteria for it to be RIPA surveillance.

6.4.2 Social Services

Social Services need to carry out investigations to protect vulnerable persons such as children. These would not be treated as criminal investigations and are normally dealt with by the Family Court. There may be occasions where some form of targeted covert surveillance activity is required to gather evidence for decision making or court proceedings. It is often the case that this type of surveillance is carried out by outside contractors. If this is the case, the above procedure for surveillance outside of RIPA should be followed in order to demonstrate that the Council has considered the activity with regard to Necessity and Proportionality and taken account of the intrusion on anyone.

6.4.3 Disciplinary Investigations

There may be serious disciplinary investigations that require some form of targeted covert surveillance activity which will engage Article 8 rights to privacy. There is specific guidance issued by the Information Commissioners Office (ICO) in the Employment Practices Code under Part 3 Monitoring at

Work. There is a link to this guidance below. This guidance makes it clear that surveillance should only be used for serious matters and that the activity must be Necessary and Proportionate taking account of the intrusion issues.

https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

6.4.4 In the above scenarios, if these issues were criminal investigations and the offences carried the required sentence of 6 months imprisonment they would meet the Directed Covert Surveillance criteria under RIPA and would require authorisation. However, these scenarios are to be treated as targeted surveillance operations outside of RIPA and the procedure for surveillance outside of RIPA should be followed in order to demonstrate that the Council has considered the activity with regard to Necessity and Proportionality and taken account of the intrusion on anyone.

6.5 Other routine activity that may be surveillance

6.5.1 There are other routine scenarios that may amount to surveillance, for example the **deployment of a noise recording machine**, which may be monitoring persons and conversations etc. In these instances, the persons responsible for the noise are notified that the recording activity may take place, which would give them a reduced expectancy of privacy. However, the Council still has an obligation to consider the intrusion issues and Necessity and Proportionality, which will include the management and disposal of any personal data obtained. Therefore, staff should carry out some form of privacy impact assessment and be able to demonstrate why it was necessary to deploy the noise machine and that it was a proportionate response to the problem to be resolved. It is likely that this can be documented and managed within the case notes of that particular complaint.

7 Internet and Social Media - use for Research and Investigations

7.1 Online open source research is widely regarded as the collection, evaluation and analysis of material from online sources available to the public, whether by payment or otherwise to use as intelligence and evidence.

7.2 The use of online open source internet and social media research techniques has become a productive method of obtaining information concerning individuals to assist the Council with its regulatory and enforcement functions. It can also assist with service delivery issues, employment matters and debt recovery. However, the use of the internet and social media is constantly evolving and there are risks associated with these types of enquiries, regarding breaches of privacy under Article 8 Human Rights Act (HRA) and other operational risks.

7.3 The activity may require RIPA authorisations for Directed Covert Surveillance or CHIS. Where this is the case, the application process and the contents of this Policy are to be followed.

- 7.4 Where the activity falls within the criteria of surveillance outside of RIPA, again this will require authorising on a non RIPA form which will be authorised internally
- 7.5 In carrying out online research and investigations in respect of individuals regard should be had to the 2018 Code Attached at Appendix 3 is the summary of the key points relating to social media from the 2018 Code In addition the Council has prepared a separate procedure note specifically dealing with the use of the Internet and Social Media for investigations

8. Use of CCTV

- 8.1 The use of the CCTV systems operated by the Council do not normally fall under RIPA However, it does fall under the Data Protection Act 2018 and the Council's CCTV Policy. Guidance on operation of CCTV is provided in the "Surveillance Camera Code of Practice" issued under the Protection of Freedoms Act 2012 ("the 2012 Act") and overseen by the Surveillance Camera Commissioner Local Authorities should also be aware of the relevant Information Commissioner's code of practice ("In the Picture – A Data Protection Code of Practice for Surveillance Cameras and Personal Information") Should there be a requirement for the CCTV cameras to be used for a specific operation to conduct surveillance it is likely that the activity will fall under directed covert surveillance and therefore require an authorisation
- 8.2 On the occasions when the CCTV cameras are used for directed covert surveillance, either by enforcement officers from relevant departments within the Council or outside Law Enforcement Agencies such as the Police, either the CCTV staff are to have a copy of the application form in a redacted format, or at least a copy of the authorisation page. It is important that the staff check the authority and only carry out what is authorised
- 8.3 Operators of the Council's CCTV system need to be aware of the RIPA issues associated with using CCTV and that continued, prolonged, systematic surveillance of an individual may require an authorisation

9 Use of material as evidence

- 9.1 Material obtained through directed covert surveillance, may be used as evidence in criminal proceedings The admissibility of evidence is governed primarily by the common law, the Criminal Procedure and Investigations Act 1996, the Civil Procedure Rules, section 78 of the Police and Criminal Evidence Act 1984 and the Human Rights Act 1998.
- 9.2 Ensuring the continuity and integrity of evidence is critical to every prosecution Accordingly, considerations as to evidential integrity are an important part of the disclosure regime under the Criminal Procedure and

Investigations Act 1996 and these considerations will apply to any material acquired through directed covert surveillance or property interference that is used in evidence. When information obtained under a directed covert surveillance authorisation is used evidentially, it will be necessary to be able to demonstrate how the evidence has been obtained, to the extent required by the relevant rules of evidence and disclosure.

10 Safeguards of Material

- 10.1 The Council and all staff should ensure that their actions when handling information obtained by means of directed covert surveillance comply with the Data Protection Act 2018, General Data Protection Regulation and the Council's Data Retention Policy and the Criminal Procedures Investigations Act 1996 (CPIA). This will ensure that any interference with privacy is justified in accordance with Article 8(2) of the European Convention on Human Rights. Compliance with these legal frameworks will ensure that the handling of private information so obtained continues to be lawful, justified and strictly controlled, and is subject to robust and effective safeguards.
- 10.2 Dissemination, copying and retention of material must be limited to the minimum necessary for authorised purposes. This obligation applies equally to disclosure to additional persons within the Council and to disclosure outside the authority.
- 10.3 Material obtained through directed covert surveillance or property interference, and all copies, extracts and summaries of it, must be handled and stored securely, so as to minimise risk. It must be held so as to be inaccessible to persons who would not need to see it (where applicable). This requirement applies to all those who are responsible for the handling of the material.
- 10.4 Any breaches of data protection requirements should be reported to the Council's DPA Officer and the SRO as it is likely to constitute an error.

11 Errors

- 11.1 Proper application of the surveillance provisions in the 2018 Codes should reduce the scope for making errors.
- 11.2 An error must be reported if it is a "relevant error". A relevant error is any error by a public authority in complying with any requirements that are imposed on it by any enactment which are subject to review by a Judicial Commissioner. This would include compliance by public authorities with Part II of the 2000 Act (RIPA).
- 11.3 Examples of relevant errors occurring would include circumstances where

- Surveillance activity has taken place without lawful authorisation.
- There has been a failure to adhere to the safeguards set out in the relevant statutory provisions and Chapter 9 of the 2018 Code relating to the safeguards of the material

11.4 Errors can have very significant consequences on an affected individual's rights. All relevant errors made by public authorities must be reported to the IPCO by the public authority that is aware of the error as soon as reasonably practicable and a full report no later than ten working days. The report should include information on the cause of the error, the amount of surveillance or property interference conducted, and material obtained or disclosed; any unintended collateral intrusion; any analysis or action taken; whether any material has been retained or destroyed, and a summary of the steps taken to prevent recurrence.

Serious Errors

- 11.5 The IPCO must inform a person of any relevant error relating to that person if the Commissioner considers that the error is a serious error and that it is in the public interest for the person concerned to be informed of the error. The Commissioner may not decide that an error is a serious error unless they consider that the error has caused significant prejudice or harm to the person concerned. The fact that there has been a breach of a person's Convention rights (within the meaning of the Human Rights Act 1998) is not sufficient by itself for an error to be a serious error.
- 11.6 It is important that all staff involved in the RIPA process report any issues so they can be assessed as to whether it constitutes an error which requires reporting

12 Complaints

- 12.1 The Investigatory Powers Tribunal (IPT) has jurisdiction to investigate and determine complaints against Local authority use of investigatory powers, including those covered by the 2018 Code, and is the only appropriate tribunal for human rights claims against the intelligence services. Any complaints about the use of powers as described in the 2018 Code should be directed to the IPT.
- 12.2 The IPT is entirely independent from Her Majesty's Government and all public authorities who use investigatory powers. It is made up of members of the judiciary and senior members of the legal profession. Following receipt of a complaint or claim from a person, the IPT can undertake its own enquiries and investigations and can demand access to all information necessary to establish the facts of a claim and to reach a determination. A 'person' for

these purposes includes an organisation, an association, or combination of persons (see section 81(1) of RIPA), as well as an individual.

- 12.3 Further information on the exercise of the Tribunal's functions and details of the relevant complaints procedure can be obtained from

Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZQ

Tel 0207 0353711

www.ipt-uk.com.

- 12.4. Notwithstanding the above, members of the public will still be able to avail themselves of the Council's internal complaints procedure, where appropriate, and can complain to the Local Government Ombudsman.

13 Oversight by the IPCO

- 13.1 The Investigatory Powers Act 2016 provides for an Investigatory Powers Commissioner ("the Commissioner"), whose remit includes providing comprehensive oversight of the use of the powers to which this Policy applies, and adherence to the practices and processes described in it. The Commissioner will be, or will have been, a member of the senior judiciary and will be entirely independent of Her Majesty's Government or any of the public authorities authorised to use investigatory powers. The Commissioner will be supported by inspectors and others, such as technical experts, qualified to assist the Commissioner in his or her work. The Commissioner will also be advised by the 'Technology Advisory Panel'.
- 13.2 One of the duties of the IPCO is to carry out planned inspections of those public authorities who carry out surveillance as specified in RIPA, to ensure compliance with the statutory authorisation procedures. At these inspections they have unfettered access to all locations, documentation and information systems as necessary to carry out their full functions and duties. All relevant persons using investigatory powers must provide all necessary assistance to the Commissioner and anyone who is acting on behalf of the Commissioner.
- 13.3 An inspection report will be presented to the Chief Executive, which should highlight any significant issues, draw conclusions and make appropriate recommendations. The aim of inspections is to be helpful rather than to measure or assess operational performance.

- 13 4 In addition to routine inspections, spot checks may be carried out from time to time.
- 13 5 There is a duty on every person who uses the powers provided by Part II of RIPA, which governs the use of directed covert surveillance or covert human intelligence sources, to disclose or provide to the Chief Commissioner (or his duly appointed Inspectors) all such documents and information that he may require for the purposes of enabling him to carry out his functions

PART 2

DETAILED PROCEDURES FOR UNDERTAKING DIRECTED COVERT SURVEILLANCE

1. Purpose

To ensure that surveillance is only undertaken in appropriate cases, is properly authorised and recorded and is compliant with the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 and appropriate Code of Practices, made there under

2 Scope

- 2 1 These procedures must be complied with by all sections and Investigating Officers, who routinely or occasionally undertake directed covert surveillance in connection with preventing or detecting crime with a maximum 6 months imprisonment or relate to the sale of alcohol or tobacco to children (the only permitted purpose for such surveillance). Local investigation procedures should make reference to this Policy

3. Procedure

- 3 1 It is very important that the correct authorisation procedure is followed prior to undertaking surveillance activity. Interference of the right to privacy without proper authorisation may render any evidence obtained unusable in a criminal court. If surveillance is conducted on individuals without the necessary authorisation, the Council and possibly individuals may be sued for damages for a breach of Human Rights. In civil matters adverse inferences may be drawn from such interference.
- 3 2 This procedure is supported by the 2018 Code. If the surveillance is not likely to obtain private information, the 2018 Code does not apply. All Investigating Officers and Authorising Officers should fully acquaint themselves with the 2018 Code and refer to it during both the application and authorisation processes.
- 3 3 All directed covert surveillance activity must be approved prior to the activity taking place by an Authorising Officer and a Justice of the Peace ("JP"). Officers seeking authority to undertake directed covert surveillance should complete the form, "Application for use of Directed Covert Surveillance". A sample application form with notes is attached at **Appendix 1**, but the latest

version from the Gov UK website must always be used. Completed application forms should be forwarded to the relevant Authorising Officer.

- 3.4 Completed authorisation forms should be allocated a reference number by the Investigating Officer relevant to the department / team and the particular investigation. The Investigating Officer should also obtain the next unique reference number from the Central Record of RIPA Applications and Authorisations maintained by the Principal Legal Executive.
- 3.5 The Authorising Officer will consider the completed application form and inform the Investigating Officer of his / her decision. The Authorising Officer will retain a copy of the authorisation form and monitor this for review, renewal and cancellation should it be approved by a JP. The original will be required to be returned to the applicant if authorised to be presented before a JP. If refused by the Authorising Officer or JP the original will be forwarded to the Principal Legal Executive for filing.
- 3.6 In addition the Authorising Officer must notify the Chief Executive of an authorisation.
- 3.7 The Investigating Officer and the Authorising Officer must give consideration to the following factors.
- **Necessity** – is covert surveillance the only or best way to achieve the desired information, or are other less invasive methods appropriate?
 - **Proportionality:**
 - balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence,
 - explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others,
 - considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result; and
 - evidencing, as far as reasonable practicable, what other methods had been considered and why they were not implemented
 - **Collateral intrusion** – that is the obtaining of information relating to persons other than the subject of the investigation and the need to minimise this.
 - **Confidential Information** - The Investigating Officer and the Authorising Officer must consider the possibility that the surveillance activity may result in the acquiring of confidential information. If this is

considered to be likely then the Investigating Officer must highlight this on the application

- 3.8 All Investigating Officers completing RIPA applications must ensure that applications are sufficiently detailed. When completing an application or authorisation, the Investigating Officer and Authorising Officer must ensure that the case for the authorisation is presented in the application in a fair and balanced way. In particular, all reasonable efforts should be made to take into account information which weakens the case for the warrant or authorisation. Authorising Officers should refuse to authorise applications that are not to the required standard and should refer them back to the Investigating Officers.
- 3.9 **Magistrates' Court Approval:** As from the 1st November 2012 all applications and renewals for Directed Covert Surveillance and use of a CHIS will be required to have a JP's approval.
- 3.10 Having had the activity authorised by the Authorising Officer, the Investigating Officer must now complete the relevant Judicial Approval form to seek approval from a JP. The Investigating Officer must ensure compliance with the statutory provisions and should refer to the Home Office publication (October 2012) "Protection of Freedoms Act 2012 – changes to provisions under the Regulation of Investigatory Powers Act 2000 (RIPA) Home Office guidance to local authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for directed surveillance"
- <https://www.gov.uk/government/publications/changes-to-local-authority-use-of-ripa>)
- 3.11 The Judicial Approval form (see **Appendix 2**) will be submitted to the JP for approval. The form requires the Investigating Officer to provide a brief summary of the circumstances of the case on the judicial application form.
- 3.12 The contact numbers for Her Majesty's Court and Tribunals Service to arrange a hearing is
- Within office hours 01245 313315 or 01245 313313
 - If out of hours the contact numbers are 07736 638551 or 07774 238418
- 3.13 At the hearing which is on oath, the officer must present to the JP.
- the partially completed judicial approval/ order form,
 - a copy of the RIPA application / authorisation form, together with any supporting documents setting out the case, and

- the original application / authorisation form (this must be retained by Investigating Officer)

It is preferred that the Authorising Officer also attends the hearing at the Magistrates' Court

- 3.14 The JP will consider the paperwork and may ask questions to clarify points or require additional reassurance on particular matters

The JP will

- Consider whether he or she is satisfied that at the time the authorisation was granted or renewed, there were reasonable grounds for believing that the authorisation was necessary and proportionate,
- Consider whether there continues to be reasonable grounds;
- Consider whether the person who granted the authorisation or gave the notice was an appropriate designated person within the Local Authority, and
- Consider whether if the authorisation was made in accordance with the law, i.e. that the crime threshold for directed covert surveillance has been met

- 3 15 The JP may:

- Decide to approve the Grant or renewal of an authorisation which will then take effect and the Local Authority may proceed to use the technique in that particular case, or
- Refuse to approve the grant or renewal of an authorisation in which case the RIPA authorisation will not take effect and the Local Authority may not use the technique in that case

- 3 16 Where an application has been refused the Investigating Officer should consider the reasons for that refusal. If more information was required by the JP to determine whether the application / authorisation has met the tests, and this is the reason for refusal, the Investigating Officer should consider whether they can reapply, for example, if there was information to support the application which was available to the Local Authority, but not included in the papers provided at the hearing.

- 3 17 Where the JP refuses to approve the application / authorisation or renew the application / authorisation and decides to quash the original authorisation or notice the court must not exercise its power to quash the application / authorisation unless the applicant has had at least 2 business days from the date of the refusal in which to make representations. If this is the case the officer will inform Legal Services who will consider whether to make any representations.

- 3 18 Whatever the decision, the JP will record their decision on the order section of the judicial application / order form. The court will retain the copy of the Local Authority RIPA application and authorisation form and the judicial application / order form. The officer will retain the original application / authorisation and a copy of the judicial application / order form
- 3 19 As previously stated the Principal Legal Executive is responsible for giving each authorisation a central unique identification number using a standard consistent format and recording it in a Central Record of RIPA Applications and Authorisations. This is to ensure that an up-to-date central record is maintained for all directed covert surveillance activity. Similarly, copies of all cancellations, renewals and review applications should be forwarded to the Principal Legal Executive promptly. The original authorisation should be kept on the investigation file
- 3 20 Written surveillance authorisations last for a maximum of three months. They cannot be authorised for a lesser period and the commencement date is the date approved by the JP. Surveillance authorisations must be cancelled when no longer required (see 3 30 below)

Reviews

- 3 21 The Authorising Officer has the responsibility to set the review dates for each authorisation and will determine what the review dates will be. The review date is detailed on the authorisation form. The review date will be at most one month from the date approved by the JP or previous review. The Authorising Officer should conduct the review with the Investigating Officer. Reviews should not be conducted solely by the Investigating Officer. Details of the review should be recorded on the form "Review of the use of Directed Surveillance Authorisation", available on the Home Office website and retained with the original authorisation. The Authorising Officer must ensure through diarisation or otherwise that reviews are conducted at the correct date
- 3 22 Any proposed or unforeseen changes to the nature or extent of the surveillance operation which may result in the further or greater intrusion into the private life of any person should be brought to the attention of the Authorising Officer by means of a review.
- 3 23 There is no requirement for a review form to be submitted to a JP. However if a different surveillance technique is required it is likely a new application will have to be completed and approved by a JP.

Renewal

- 3.24 Should it be necessary to renew a Directed Covert Surveillance or CHIS application / authorisation, this must be approved by a JP

- 3 25 Applications for renewals should not be made until shortly before the original authorisation period is due to expire but the applicant must take account of factors which may delay the renewal process (e.g. intervening weekends or the availability of the relevant authorising officer and a JP to consider the application)
- 3 26 The applicant should complete all the sections within the renewal form and submit the form to the Authorising Officer
- 3 27 Authorising Officers should examine the circumstances with regard to Necessity, Proportionality and the Collateral Intrusions issues before making a decision to renew the activity. A CHIS application should not be renewed unless a thorough review has been carried out covering the use made of the source, the tasks given to them and information obtained. The Authorising Officer must consider the results of the review when deciding whether to renew or not. The review and the consideration must be documented.
- 3 28 If the Authorising Officer refuses to renew the application the cancellation process should be completed. If the Authorisation Officer authorises the renewal of the activity the same process is to be followed as mentioned earlier for the initial application.

A renewal takes effect on the day on which the authorisation would have ceased and lasts for a further period of three months.

Cancellation

- 3 29 The Investigating Officer must complete the "Cancellation of the use of Directed Covert Surveillance" form available on the Home Office website and forward to the Authorising Officer who granted or last renewed the authorisation. It must be cancelled if they are satisfied that the directed covert surveillance no longer meets the criteria upon which it was authorised. Where the Authorising Officer is no longer available, this duty will fall on the person who has taken over the role of Authorising Officer or the person who is acting as Authorising Officer.
- 3 30 As soon as the decision is taken that directed covert surveillance should be discontinued, the applicant or other investigating officer involved in the investigation should inform the Authorising Officer. The Authorising Officer will formally instruct the Investigating Officer to cease the surveillance, noting the time and date of their decision. This will be required for the cancellation form. The date and time when such an instruction was given should also be recorded in the Central Record of RIPA Applications and Authorisations along with a note of the amount of time spent on the surveillance.
- 3 31 The officer submitting the cancellation must complete in detail the relevant sections of the form and include the period of surveillance and if any images were obtained and any images containing third parties. The Authorising

Officer must then take this into account and issues instructions regarding the management and disposal of the images etc

- 3 32 The cancellation process should also be used to evaluate whether the objectives have been achieved and whether the applicant carried out what they stated was necessary in the application form. This check will form part of the oversight function. Where issues are identified they will be brought to the attention of the line manager and the Senior Responsible Officer. This will assist with future audits and oversight

4. Joint Agency Surveillance

- 4 1 In cases where one agency is acting on behalf of another, it is usually for the lead agency to obtain or provide the authorisation subject to 4 2 below. For example, where surveillance is carried out by Council employees on behalf of the Police, authorisation would be sought by the Police. If it is a joint operation involving both agencies the lead agency should seek authorisation. Council staff involved with joint agency surveillance are to ensure that all parties taking part are authorised on the authorisation page of the application to carry out the activity and at all times their line manager must be made aware of the joint surveillance. When Council staff are operating on another organisation's authorisation they should obtain either a copy of the application form (redacted if necessary) or a copy of the authorisation, containing the unique number. This will ensure they see what activity they are authorised to carry out. They should also inform the Senior Responsible Officer or the Principal Legal Executive of the unique reference number, the agencies involved and the name of the officer in charge of the surveillance.

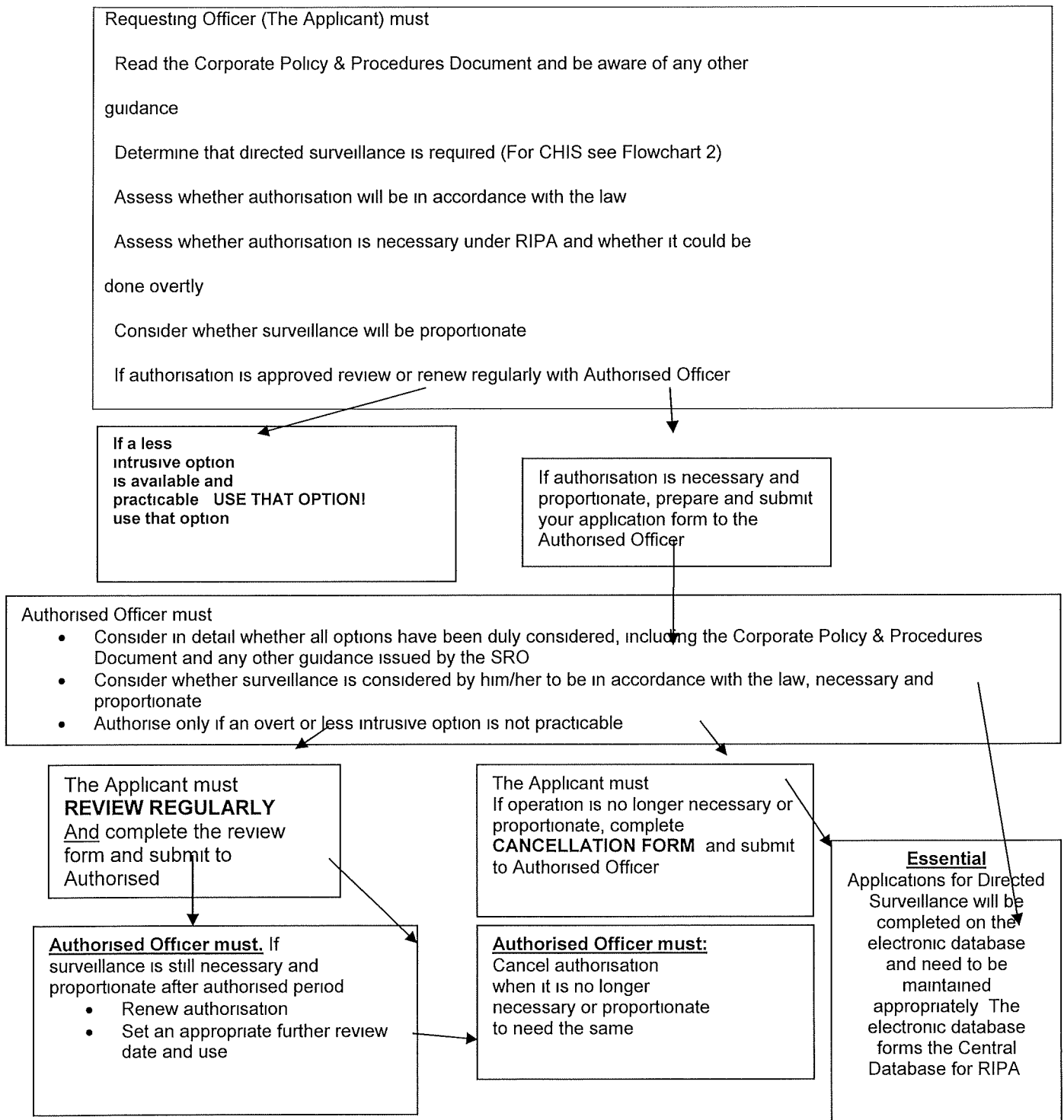
Commissioned Services

- 4 2 If the Council commissions another Local Authority to undertake investigatory services on its behalf and directed covert surveillance or the use of a CHIS is required, then that other Local Authority will normally obtain the necessary authorisation under its RIPA procedures including making application to the Magistrates' Court. The other Local Authority must supply the Council with a copy of the authorisation form.

PART 3
DETAILED PROCEDURES FOR USE OF COVERT
HUMAN INTELLIGENCE SOURCES (CHIS)

- 1 1 RIPA covers the activities of Covert Human Intelligence Sources (CHIS) which relates not only to sources commonly known as informants (members of the public providing the Council with information), but also the activities of undercover officers. It matters not whether they are employees of the Council, agents or members of the public engaged by the Council to establish or maintain a covert relationship with someone to obtain information. However, not all human intelligence source activity will meet the definition of a CHIS. For example, a source may be a public volunteer or someone who discloses information out of professional or statutory duty or has been tasked to obtain information other than by way of a covert relationship.
- 1 2 Recognising when a source becomes a CHIS is important as this type of activity may need authorisation.
- 1 3 There is a separate CHIS Policy which provides advice as to when someone is a CHIS and requires authorisation under RIPA together with the requirements involved in the process.
- 1 4 Should a CHIS authority be required, all of the staff involved in the process should make themselves fully aware of all of the CHIS Codes of Practice.
- 1 5 Legal advice should always be sought where consideration is given to the use of CHIS.

RIPA FLOW CHART 1 : DIRECTED SURVEILLANCE



NB if in doubt, ask the Group Manager (Legal and Democratic) BEFORE any directed surveillance and/or CHIS is authorised, reviewed, renewed, cancelled, or rejected.

Appendix 1 (b)

SAMPLE APPLICATION FORM FOR USE OF DIRECTED COVERT SURVEILLANCE

| | |
|--------------------------------|---|
| Unique Reference Number | Refer to your policy as to how you obtain the unique number. All applications must have one and put on each page. |
|--------------------------------|---|

Part II of the Regulation of Investigatory Powers Act 2000

Authorisation Directed Surveillance

| | | | |
|---|--|------------------------------|------------------------|
| Public Authority (including full address) | State your Public Authority Name and full address | | |
| | | | |
| Name of Applicant | Details of the person completing the form | Unit/Branch /Division | Section and department |
| Full Address | Provide the address of your department | | |
| Contact Details | Provide full contact details including email address. Make it easy for the Authorising Officer, or anyone else associated with the process to contact you. | | |
| Investigation/Operation Name (if applicable) | This may be an investigation reference number allocated to this case, or some other reference | | |
| Investigating Officer (if a person other than the applicant) | If the form is being completed by someone who is not the investigator, then the investigators details must be put in this box. | | |

DETAILS OF APPLICATION

1. Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 No. 521.¹

As above.

For local authorities: The exact position of the authorising officer should be given. For example, Head of Trading Standards.

Also use the description of the person's position contained within your policy to remove any confusion.

2. Describe the purpose of the specific operation or investigation.

Describe the investigation to date including the offences and the relevant legislation. When, where and how are the offences occurring. Remember the Authorising Officer needs to be clear what the offence is and the circumstances. (keep information relevant and to the point)

Include the details of the suspects and persons involved and the role they play within the investigation. (Do not put confidential information in such as informants' names)

Consider disclosure implications under CPIA with regards to not revealing unnecessary information. However, the AO needs sufficient relevant information to make a decision. The provisions of using CPIA sensitive information may be a way of dealing with the sensitivity issues later, by editing material if it has to be disclosed. However, if the document contains sensitive information remember to keep it secure at all times.

Cross reference where necessary to other relevant applications

3. Describe in detail the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment (e.g. camera, binoculars, recorder) that may be used.

This should be completed, after attending the area of where the activity is to be carried out, and having carried out a surveillance assessment having taken into account risks or limiting factors. Limiting factors are anything can affect the success of the operation.

Consider the AO statement in box 12, the 5 WH. The applicant can only do what is authorised by the AO, not what they have applied for.

Consider the aims and objectives, confirmation of address may only need static observations; however, lifestyle intelligence may require foot/mobile and use of covert cameras etc.

What exactly do you want to do? Is it static observations, foot or mobile? You want a combination? However, only ask for what you can realistically carry out. It is not a wish list; it should be carried out to achieve the objectives.

How do you want to carry out the surveillance and what equipment do you want to use? You must make the AO aware of the capabilities of any equipment you want to use.

¹ For local authorities. The exact position of the authorising officer should be given. For example, Head of Trading Standards

Where is the activity to take place? Who is the activity against and when do you want to carry it out?

What is the expected duration? It does not mean that it must only be authorised to this point. Once signed, the authorisation lasts for a 3 month period. You must update the AO when they set the review dates. If your operation ends prior to any review date or the 3 month period, you must cancel it straight away and submit the cancellation form. It does not expire.

REMEMBER YOU CAN ONLY DO WHAT IS AUTHORISED ON THE AO SECTION, NOT WHAT YOU HAVE APPLIED FOR IN THIS SECTION.

4. The identities, where known, of those to be subject of the directed surveillance.

- Name:
- Address:
- DOB:
- Other information as appropriate:

If you do not know who the subjects are, insert any descriptions you may have. If as a result of the surveillance, you identify anyone, you must submit this information on a review form to the AO.

Consider any known associates. If the intelligence is that the subject of the surveillance has known associates, are they likely to become subjects of the surveillance? If so, detail them as part of the application.

5. Explain the information that it is desired to obtain as a result of the directed surveillance.

These are the surveillance objectives. They should have been identified during the planning stage and a feasibility study carried out to assess whether they can be achieved. It's no use setting objectives that can't be achieved.

What is the surveillance going to tell you?

What, if any, criminality will it establish?

Will it identify subjects involved in criminality?

Will it house subject or their criminal associates?

E.G.

- Identify the location of the subject's place of work
- To gather intelligence and evidence to establish the extent of the criminality (size).
- Identify other persons involved, such as suppliers.
- Identify other premises involved, such as storage buildings.
- Obtain best evidence through the use of photographic equipment to assist with identifying the offenders
-

Obtain best evidence to assist with a prosecution of offenders

6. Identify on which grounds the directed surveillance is necessary under Section 28(3) of RIPA. Delete those that are inapplicable. Ensure that you know which of these grounds you are entitled to rely on (SI 2010 No.521).

- In the interests of national security;

- For the purpose of preventing or detecting crime or of preventing disorder;
- In the interests of the economic well-being of the United Kingdom;
- In the interests of public safety;
- For the purpose of protecting public health;
- For the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;

For Directed Surveillance, Local Authorities only lawful purpose is preventing or detecting crime and the crime must be capable of carrying six months imprisonment or criminal offences relating to the underage sale of alcohol or tobacco under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933.

Due to the nature of the offences, if any other areas above are applicable such as protection of public health, this should be made clear in the body of the application and the proportionality section.

7. Explain why this directed surveillance is necessary on the grounds you have identified [Code paragraph 3.3].

You can reiterate the criminal offences

Why is it necessary at this stage of the enquiry to carry out covert activity?

What is the purpose of the operation?

How will the activity assist or progress the investigation?

What will be the consequences of the proposed action be to the victim?

Why do we need this evidence/intelligence/information?

What other enquiries have been carried out and results? This does not have to be a last resort, but if there is a less intrusive way of achieving your objectives you should take that option, or explain why you can't take that option.

Consequences of not taking action

It is not for the applicant to state on the application that they believe it to be necessary. This is the responsibility of the AO to reach that decision.

8. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. [Bear in mind Code paragraphs 3.8 to 3.11.]

Describe precautions you will take to minimise collateral intrusion.

There are three parts to this section (see above). You must answer them all, as this section directly impacts upon the proportionality test.

1. SUPPLY DETAILS OF POTENTIAL COLLATERAL INTRUSION

Visit the location of where the activity is to take place and carry out a risk assessment. Who lives at the property that you may be watching. Have they got children who might be affected such as going to school etc.?

Determine where you need to be to carry out the surveillance. What else can you see?

What equipment will you be using and what will it see and record?

Consider Confidential Information

It may be useful to paint the picture in words of what it is you will be watching in the locality. This will assist the AO. You may also want to refer to any plans or maps attached to the application.

2. WHY IS THE INTRUSION UNAVOIDABLE?

Consider why the intrusion is unavoidable, such as the location and time frame that the observations have to be carried out. It may be that you are limited to the use of certain equipment only and therefore governed by its operating capabilities. Your observation position may be the only place you can use.

3. DESCRIBE THE PRECAUTIONS YOU WILL TAKE TO MINIMISE COLLATERAL INTRUSION

Having carried out the risk assessment and identified what the intrusion is, consider ways of reducing the intrusion, or keeping it to a minimum. You should consider:

State who the activity will be focused on, such as the subject etc., not the innocent third parties subject to the collateral intrusion.

Keeping the surveillance activity focussed with regards to length of time spent on the observations. However, remember that you still need time to achieve your objectives. You will need some flexibility built in to your timings.

If using technical equipment such as video or covert recordings, consider the position and focal length of the lenses when filming to reduce the intrusion. Consider when and who you will use the equipment against, such as the suspects only.

How will you manage any images obtained? Consider Data Protection, confidentiality, security, dissemination of the images, and any guidance provided by your organisation, including any Home Office guidance.

Are the staff trained to carry out the activity? If so, this may assist, as they should know what they are doing with regards to collateral intrusion.

The activity needs to be tightly managed and reviewed constantly. If there is a considerable change in the intrusion once the activity commences, then the AO needs to be made aware.

9. Explain why this directed surveillance is proportionate to what it seeks to achieve. How intrusive might it be on the subject of surveillance or on others? And why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means [Code paragraphs 3.4 to 3.7]?

In the necessity box we stated why it was necessary to carry out the covert activity. In this box we are assessing whether the actions requested are proportionate to the overall operational aims within the investigation, having taken into account of the intrusion issues.

How serious are the offences under investigation? What is the direct or accumulative consequence of the offences?

What are the effects of the offences on the victim or the consequences of what is happening?

Are you asking to do a lot to achieve a little? Do not use a sledgehammer to crack the nut. If you have provided a good explanation of how the intrusion will be reduced and managed in the collateral intrusion box, refer them to it.

Explain why you need to undertake this activity to achieve your objectives, against using other methods. Why, in operational terms, does your need to use the activity (how the activity will progress the investigation) outweigh the level of intrusion? Why is this method the least intrusive option?

**Are your methods/tactics balanced in relation to the likely results?
Consider the length of time of the surveillance operation**

What methods are required to achieve the objectives and are there any less intrusive methods? You should explain what if any less intrusive methods have been considered. If they can be used they should be. If however less intrusive methods cannot be used, explain why. You should also take account that technical surveillance may be more intrusive.

Consequences of not taking action.

**10. Confidential information [Code paragraphs 4.1 to 4.31].
INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL INFORMATION:**

Is there any likelihood of Health, Solicitors, Counselling, and Spiritual etc.

It is unlikely that you will obtain this type of material, but an assessment should take place. If you are, it is a higher level of Authorising Officer who needs to consider it.

Do not mix this up with Private Information which is part of the consideration when assessing whether the activity falls under RIPA.

11. Applicant's Details

| | | | |
|----------------------|--|----------------|--|
| Name (print): | | Tel No: | |
| Grade/Rank | | Date: | |
| Signature | | | |

12. Authorising Officer's Statement. [Spell out the "5 Ws" – Who; What; Where; When; Why and HOW– in this and the following box.]

I hereby authorise directed surveillance defined as follows [Why is the surveillance necessary, whom is the surveillance directed against, Where and When will it take place, What surveillance activity/equipment is sanctioned, How is it to be achieved?]

REMEMBER THAT EACH CASE HAS TO BE ASSESSED ON ITS OWN MERITS.

Who are you authorising to carry out the activity? Are the staff from one office? Or if a joint operation, please state that fact and name the other organisation. You have to actually authorise the other organisation's staff in writing.

What are you authorising them to do and what equipment are you authorising them to use? You

should have a knowledge of the equipment's capability.

Who are you authorising them to do it against, person, address, vehicle, etc?

When are you authorising them to do it?

Where are you authorising the activity to take place?

Why are you authorising whatever you are allowing them to do? They should have stated within the application earlier what they are hoping to achieve.

When authorising the activity, it is live for 3 months. In other words, as an AO, you cannot authorise for less. You should set a review date for you to review it if you think that the surveillance should be a shorter period.

DO NOT BE AFRAID AS AN AO, TO ONLY ALLOW THEM TO UNDERTAKE CERTAIN ACTIVITY, AS OPPOSED TO ALL THE ACTIVITY APPLIED FOR, IF IT MEANS THAT IT IS PROPORTIONATE. STATE WHY ON THE FORM

IF NOT AUTHORISING, STATE WHY.

13. Explain why you believe the directed surveillance is necessary [Code paragraph 3.3].
Explain why you believe the directed surveillance to be proportionate to what is sought to be achieved by carrying it out [Code paragraphs 3.4 to 3.7].

IF YOU ARE WRITING IN THIS SECTION, PRINT THE FORM OUT WITH ENOUGH SPACE TO WRITE IN. YOU WILL REQUIRE SOME SPACE TO DETAIL HOW YOU HAVE COME TO YOUR DECISION.

Below are 5 areas that should be dealt with by the AO when considering the application.

Code 3.3 requires that the person granting an authorisation BELIEVES that the authorisation is necessary in the circumstances of the particular case for one of the statutory reasons (see box 6). Have they made clear what the offence or offences are in the body of the application?

Code 3.4 then if the activities are necessary, the person granting the authorisation must BELIEVE that they are proportionate to what is sought to be achieved by carrying them out. AO must also BELIEVE that the objectives can't be met by other less intrusive means.

Sec 72 RIPA 2000, a person exercising or performing any power or duty in relation to which provision may be made by a code of practice under section 71 shall, in doing so, HAVE REGARD TO THE PROVISIONS (so far as they are applicable) of every code of practice for the time being in force under that section. (You have to know what the codes say).

Collateral Intrusion Code of Practice 3.8 before authorising surveillance the authorising officer should also TAKE INTO ACCOUNT the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation.

Code of Practice 3.15 .Any person granting or applying for an authorisation will also NEED TO BE AWARE OF particular sensitivities in the local community where the surveillance is taking place and of similar activities being undertaken by other public authorities which could impact on the deployment of surveillance.

This will take some consideration. Read and study the application fully. Refer to the applicants boxes that deal with these issues.

Detail your thought processes. How have you come to the conclusion? Do not rubber stamp, do not use template or cut and paste answers. This is your original note that you may be relying on in

court. If you are making decisions from reading supporting material, mention the material and keep a copy which needs to be part of the central register. Be careful to make your decisions on written material not discussions with the case officer which may be difficult to justify at a later date at court.

Model answer from codes and OSC

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- explaining how and why the methods to be adopted will cause the least possible intrusion on the target and others;
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

14 (Confidential Information Authorisation.) Supply detail demonstrating compliance with Code paragraphs 4.1 to 4.31.

This is completed by the AO who has the responsibility to consider the authorisation if confidential information is likely to be obtained. (Usually someone of a much higher position than a normal AO.) e.g. In a Local Authority it will be the Chief Executive.

See rear of codes of practice for relevant position and refer to your policy.

Date of first review

AO must set the review date. Consider what the applicant has stated regarding the length of time required. Remember, this is so you as the AO can now review the need for the activity to continue on the date you have set. Also refer to policy. Most state that it must not be longer than a month. However, you must assess it against all the facts.

Programme for subsequent reviews of this authorisation: [Code paragraph 3.23]. Only complete this box if review dates after first review are known. If not or inappropriate to set additional review dates then leave blank.

As above.

| | | | |
|---|--|--|--|
| Name (Print) | | Grade / Rank | |
| Signature | | Date and time | |
| Expiry date and time [e.g.: authorisation granted on 1 April 2005 - expires on 30 June 2005, 23.59] | | From 1 Nov 12 this date will be from when a Magistrate approves it. Put in the expiry date. Remember it lasts for 3 months once signed (see opposite) | |

- 15 Urgent Authorisation [Code paragraph 5.9]: Authorising officer: explain why you considered the case so urgent that an oral instead of a written authorisation was given.

OSC guidance states that there is no longer a requirement to complete the whole application form; contemporaneous notes should have been made by both applicant and AO. However, check what your policy says as some organisations still require at least this part to be completed with certain other sections. If your policy does not make it clear, seek advice.

FROM 1 NOVEMBER 2012 THERE WILL BE NO URGENT PROVISIONA AVAILABLE FOR LOCAL AUTHORITIES

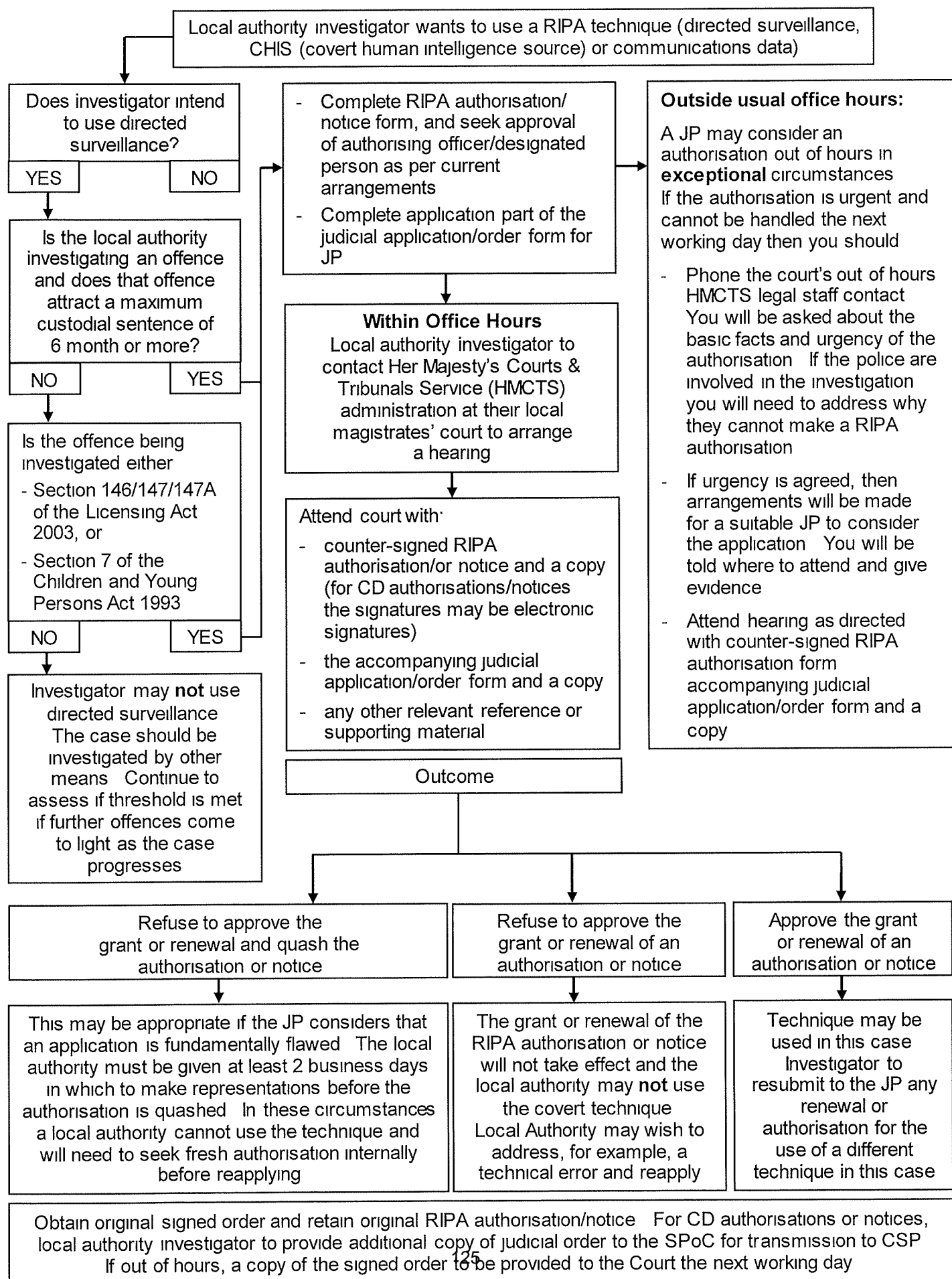
- 16 If you are only entitled to act in urgent cases: explain why it was not reasonably practicable for the application to be considered by a fully qualified authorising officer.

This is because the legislation allows for a lower rank/grade to authorise in urgent cases for some organisations. Refer to your policy.

See Statutory Instrument 2010 No 521.

| | | | |
|---|--|---------------|--|
| Name (Print) | | Grade/ Rank | |
| Signature | | Date and Time | |
| Urgent authorisation Expiry date: | | Expiry time: | |
| <i>Remember the 72 hour rule for urgent authorities – check Code of Practice.</i> | e g. authorisation granted at 5pm on June 1 st expires 4 59pm on 4 th June | | |

LOCAL AUTHORITY PROCEDURE: APPLICATION TO A JUSTICE OF THE PEACE SEEKING AN ORDER TO APPROVE THE GRANT OF A RIPA AUTHORISATION OR NOTICE



COPY APPLICATION FORM AND ORDER FOR JUDICIAL APPROVAL

Application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.

Local authority:
 Local authority department:.....
 Offence under investigation:.....
 Address of premises or identity of subject

Covert technique requested: (tick one and specify details)

Communications Data ☐
 Covert Human Intelligence Source ☐
 Directed Surveillance ☐

Summary of details

.....

Note: this application should be read in conjunction with the attached RIPA authorisation/RIPA application or notice

Investigating Officer
 Authorising Officer/Designated Person:
 Officer(s) appearing before JP:
 Address of applicant department:.....

 Contact telephone number:
 Contact email address (optional)
 Local authority reference:
 Number of pages:

Order made on an application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.

Magistrates' court:.....

Having considered the application, I (tick one):

- ☐ am satisfied that there are reasonable grounds for believing that the requirements of the Act were satisfied and remain satisfied, and that the relevant conditions are satisfied and I therefore approve the grant or renewal of the authorisation/notice.
- ☐ refuse to approve the grant or renewal of the authorisation/notice
- ☐ refuse to approve the grant or renewal and quash the authorisation/notice.

Notes

.....

.....

.....

.....

.....

Reasons

.....

.....

.....

.....

.....

.....

Signed

Date:

Time:

Full name.

Address of magistrates' court:



Summary of the key points relating to Social Media from the

Covert Surveillance and Property Interference Revised Code of Practice August 2018

Online Covert Activity (Directed Surveillance Codes Aug 18)

3.4 Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by a public authority of that person's activities for future consideration or analysis. Surveillance of publicly accessible areas of the internet should be treated in a similar way, recognising that there may be an expectation of privacy over information which is on the internet, particularly where accessing information on social media websites. See paragraphs 3.10 to 3.17 below for further guidance about the use of the internet as a surveillance tool

3.10 The growth of the internet, and the extent of the information that is now available online, presents new opportunities for public authorities to view or gather information which may assist them in preventing or detecting crime or carrying out other statutory functions, as well as in understanding and engaging with the public they serve. It is important that public authorities are able to make full and lawful use of this information for their statutory purposes. Much of it can be accessed without the need for RIPA authorisation, use of the internet prior to an investigation should not normally engage privacy considerations. But if the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, RIPA authorisations may need to be considered. The following guidance is intended to assist public authorities in identifying when such authorisations may be appropriate.

3.11 The internet may be used for intelligence gathering and/or as a surveillance tool. Where online monitoring or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private information about a person or group, an authorisation for directed surveillance should be considered, as set out elsewhere in this code. Where a person acting on behalf of a public authority is intending to engage with others online without disclosing his or her identity, a CHIS authorisation may be needed (paragraphs 4.10 to 4.16 of the Covert Human Intelligence Sources code of practice provide detail on where a CHIS authorisation may be available for online activity).

3.12 In deciding whether online surveillance should be regarded as covert, consideration should be given to the likelihood of the subject(s) knowing that the surveillance is or may be taking place. Use of the internet itself may be

considered as adopting a surveillance technique calculated to ensure that the subject is unaware of it, even if no further steps are taken to conceal the activity. Conversely, where a public authority has taken reasonable steps to inform the public or particular individuals that the surveillance is or may be taking place, the activity may be regarded as overt and a directed surveillance authorisation will not normally be available.

3.13 As set out in paragraph 3.14 below, depending on the nature of the online platform, there may be a reduced expectation of privacy where information relating to a person or group of people is made openly available within the public domain, however in some circumstances privacy implications still apply. This is because the intention when making such information available was not for it to be used for a covert purpose such as investigative activity. This is regardless of whether a user of a website or social media platform has sought to protect such information by restricting its access by activating privacy settings.

3.14 Where information about an individual is placed on a publicly accessible database, for example the telephone directory or Companies House, which is commonly used and known to be accessible to all, they are unlikely to have any reasonable expectation of privacy over the monitoring by public authorities of that information. Individuals who post information on social media networks and other websites whose purpose is to communicate messages to a wide audience are also less likely to hold a reasonable expectation of privacy in relation to that information.

3.15 Whether a public authority interferes with a person's private life includes a consideration of the nature of the public authority's activity in relation to that information. Simple reconnaissance of such sites (i.e. preliminary examination with a view to establishing whether the site or its contents are of interest) is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation. But where a public authority is systematically collecting and recording information about a particular person or group, a directed surveillance authorisation should be considered. These considerations apply regardless of when the information was shared online. See also paragraph 3.6

3.6 Private information may include personal data, such as names, telephone numbers and address details. Where such information is acquired by means of covert surveillance of a person having a reasonable expectation of privacy, a directed surveillance authorisation is appropriate¹³

Example 1. A police officer undertakes a simple internet search on a name, address or telephone number to find out whether a subject of interest has an online presence. This is unlikely to need an authorisation. However, if having found an individual's social media profile or identity, it is decided to monitor it or extract information from it for retention in a record because it is relevant to an investigation or operation, authorisation should then be considered.

Example 2. A customs officer makes an initial examination of an individual's online profile to establish whether they are of relevance to an investigation. This is unlikely to need an authorisation. However, if during that visit it is intended to extract and record information to establish a profile including information such as identity, pattern of life, habits, intentions or associations, it may be advisable to have in place an authorisation even for that single visit. (As set out in the following paragraph, the purpose of the visit may be relevant as to whether an authorisation should be sought.)

Example 3: A public authority undertakes general monitoring of the internet in circumstances where it is not part of a specific, ongoing investigation or operation to identify themes, trends, possible indicators of criminality or other factors that may influence operational strategies or deployments. This activity does not require RIPA authorisation. However, when this activity leads to the discovery of previously unknown subjects of interest, once it is decided to monitor those individuals as part of an ongoing operation or investigation, authorisation should be considered.

3.16 In order to determine whether a directed surveillance authorisation should be sought for accessing information on a website as part of a covert investigation or operation, it is necessary to look at the intended purpose and scope of the

online activity it is proposed to undertake. Factors that should be considered in establishing whether a directed surveillance authorisation is required include:

- Whether the investigation or research is directed towards an individual or organisation;
- Whether it is likely to result in obtaining private information about a person or group of people (taking account of the guidance at paragraph 3.6 above);
- Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile;
- Whether the information obtained will be recorded and retained;
- Whether the information is likely to provide an observer with a pattern of lifestyle;
- Whether the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life,
- Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s),
- Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and therefore constitute collateral intrusion into the privacy of these third parties

3.17 Internet searches carried out by a third party on behalf of a public authority, or with the use of a search tool, may still require a directed surveillance authorisation (see paragraph 4.32).

Example: Researchers within a public authority using automated monitoring tools to search for common terminology used online for illegal purposes will not normally require a directed surveillance authorisation. Similarly, general analysis of data by public authorities either directly or through a third party for predictive purposes (e.g. identifying crime hotspots or analysing trends) is not usually directed surveillance. In such cases, the focus on individuals or groups is likely to be sufficiently cursory that it would not meet the definition of surveillance. But officers should be aware of the possibility that the broad thematic research may evolve, and that authorisation may be appropriate at the point where it begins to focus on specific individuals or groups. If specific names or other identifiers of an individual or group are applied to the search or analysis, an authorisation should be considered.

Internet and Urgent Enquires

Example: An authorisation under the 2000 Act would not be appropriate where police officers conceal themselves to observe suspicious persons that they come across in the course of a routine patrol or monitor social media accounts during a public order incident.

General Observations

3.33 The general observation duties of many law enforcement officers and other public authorities do not require authorisation under the 2000 Act, whether covert or overt. Such general observation duties frequently form part of the legislative functions of public authorities, as opposed to the pre-planned surveillance of a specific person or group of people. General observation duties may include monitoring of publicly accessible areas of the internet in circumstances where it is not part of a specific investigation or operation.

Collateral Intrusion

4.14 In order to give proper consideration to collateral intrusion, an authorising officer or person considering issuing the warrant should be given full information regarding the potential scope of the anticipated surveillance or interference, including the likelihood that any equipment or software deployed may cause intrusion on persons or property other than the subject(s) of the application. If an automated system such as an online search engine is used to obtain the information, the authorising officer should be made aware of its potential extent and limitations. Material which is not necessary or proportionate to the aims of the operation or investigation should be discarded or securely retained separately where it may be required for future evidential purposes. The authorising officer or person considering issuing the warrant should ensure appropriate safeguards for the handling, retention or destruction of such material in accordance with chapter 9 of this code, as well as compliance with data protection requirements

4.15 Where it is proposed to conduct surveillance activity or property interference specifically against individuals who are not suspected of direct or culpable involvement in the overall matter being investigated, interference with the privacy or property of such individuals should not be considered as collateral intrusion but rather as intended intrusion. Any such surveillance or property interference activity should be carefully considered against the necessity and proportionality criteria

4.16 Where a public authority intends to access a social media or other online account to which they have been given access with the consent of the owner, the authority will still need to consider whether the account(s) may contain information about others who have not given their consent. If there is a likelihood of obtaining private information about others, the need for a directed surveillance authorisation should be considered, particularly (though not exclusively) where it is intended to monitor the account going forward

Example: If an individual provides the police with passwords and log-in details for their personal social networking accounts in order to provide evidence of threats made against them, this would not normally require a directed surveillance authorisation. If the police then decided to monitor the accounts for the purposes of obtaining further evidence of criminal activity by the author of the threats, they should consider applying for a directed surveillance authorisation in circumstances where private information is likely to be obtained. This is because the police would be acting with the intention to monitor an individual who has not consented to and may not be aware of the surveillance. The public authority will also need to consider the extent of the collateral intrusion into the privacy of others who may comment on or post information onto the accounts under surveillance.

Use of a Third Party

4.32 In some circumstances it may be appropriate or necessary for a public authority to work with third parties who are not themselves a public authority (such as an individual, company or non-governmental organisation) to assist with an investigation. Where that third party is acting in partnership with or under the direction of a public authority, then they are acting as an agent of that authority and any activities that third party conducts which meet the 2000 Act definitions of directed or intrusive surveillance or amount to property interference for the purposes of the 1994 or 1997 Act, should be considered for authorisation under those Acts by the public authority on whose behalf that activity is being undertaken. Similarly, a surveillance authorisation should also be considered where the public authority is aware that a third party (that is not a public authority) is independently conducting surveillance and the public authority intends to make use of any suitable material obtained by the third party for the purposes of a specific investigation being undertaken by that public authority

CHIS Codes Aug 18

Online Covert Activity

4.11 Any member of a public authority, or person acting on their behalf, who conducts activity on the internet in such a way that they may interact with others, whether by publicly open websites such as an online news and social networking

service, or more private exchanges such as e-messaging sites, in circumstances where the other parties could not reasonably be expected to know their true identity (as an official rather than private individual), should consider whether the activity requires a CHIS authorisation. A directed surveillance authorisation should also be considered, unless the acquisition of that information is or will be covered by the terms of an applicable CHIS authorisation.

4.12 Where someone, such as an employee or member of the public, is tasked by a public authority to use an internet profile to establish or maintain a relationship with a subject of interest for a covert purpose, or otherwise undertakes such activity on behalf of the public authority, in order to obtain or provide access to information, a CHIS authorisation is likely to be required.

For example:

- An investigator using the internet to engage with a subject of interest at the start of an operation, in order to ascertain information or facilitate a meeting in person.
- Directing a member of the public (such as a CHIS) to use their own or another internet profile to establish or maintain a relationship with a subject of interest for a covert purpose.
- Joining chat rooms with a view to interacting with a criminal group in order to obtain information about their criminal activities.

4.13 A CHIS authorisation will not always be appropriate or necessary for online investigation or research. Some websites require a user to register providing personal identifiers (such as name and phone number) before access to the site will be permitted. Where a member of a public authority sets up a false identity for this purpose, this does not in itself amount to establishing a relationship, and a CHIS authorisation would not immediately be required, though consideration should be given to the need for a directed surveillance authorisation if the conduct is likely to result in the acquisition of private information, and the other relevant criteria are met.

Example 1: An HMRC officer intends to make a one-off online test purchase of an item on an auction site, to investigate intelligence that the true value of the goods is not being declared for tax purposes. The officer concludes the purchase and does not correspond privately with the seller or leave feedback on the site. No covert relationship is formed and a CHIS authorisation need not be sought.

Example 2: HMRC task a member of the public to purchase goods from a number of websites to obtain information about the identity of the seller, country of origin of the goods and banking arrangements. The individual is required to engage with the seller as necessary to complete the purchases. The deployment should be covered by a CHIS authorisation because of the intention to establish a relationship for covert purposes.

4.14 Where a website or social media account requires a minimal level of interaction, such as sending or receiving a friend request before access is permitted, this may not in itself amount to establishing a relationship. Equally, the use of electronic gestures such as “like” or “follow” to react to information posted by others online would not in itself constitute forming a relationship. However, it should be borne in mind that entering a website or responding on these terms may lead to further interaction with other users and a CHIS authorisation should be obtained if it is intended for an officer of a public authority or a CHIS to engage in such interaction to obtain, provide access to or disclose information.

Example 1: An officer maintains a false persona, unconnected to law enforcement, on social media sites in order to facilitate future operational research or investigation. As part of the legend building activity he “follows” a variety of people and entities and “likes” occasional posts without engaging further. No relationship is formed and no CHIS authorisation is needed.

Example 2: The officer sends a request to join a closed group known to be administered by a subject of interest, connected to a specific investigation. A directed surveillance authorisation would be needed to cover the proposed covert monitoring of the site. Once accepted into the group it becomes apparent that further interaction is necessary. This should be authorised by means of a CHIS authorisation

4.15 When engaging in conduct as a CHIS, a member of a public authority should not adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without considering the need for authorisation. Full consideration should be given to the potential risks posed by that activity.

4.16 Where use of the internet is part of the tasking of a CHIS, the risk assessment carried out in accordance with section 6.13 of this code should include consideration of the risks arising from that online activity including factors such as the length of time spent online and the material to which the CHIS may be exposed. This should also take account of any disparity between the technical skills of the CHIS and those of the handler or authorising officer, and the extent to which this may impact on the effectiveness of oversight.

4.17 Where it is intended that more than one officer will share the same online persona, each officer should be clearly identifiable within the overarching authorisation for that operation, providing clear information about the conduct required of each officer and including risk assessments in relation to each officer involved. (See also paragraph 3.23)

5.29 Where an over-arching authorisation has been provided as a framework for investigators to establish an online presence intended to provide a basis for future enforcement activity, this should be treated as part of the same investigation or operation for renewal purposes. However, where this generic activity leads to a separate operation against subjects identified through the online presence, a fresh authorisation should be considered, and a decision taken on a case by case basis by reference to the factors listed in paragraph 5.28 above.

OSC procedures & Guidance 2016

76. To assist an Authorising Officer to reach a proper judgment, the value of the data, information or intelligence on which the application has been made should be clear. It is considered best practice for law enforcement agencies to utilise standard evaluation nomenclature which grades both the source and the information. While it is not necessary or desirable in the application to spell out in detail the content of intelligence logs, cross-referencing to these enables an Authorising Officer to check detail. Particular care should be taken when using data or information obtained from open or unevaluated sources such as the Internet or social networks.

243. Covert Internet Investigators (now often referred to as undercover officers on line (UCOL)) may establish or maintain a relationship with more than one individual in relation to different investigations. If it is not possible to construct a single authorisation to cover all of the relationships (because the persons with whom relationships are established are not known in advance) it will be necessary to construct for each person with whom a relationship has been established a separate authorisation each of 12 months' duration. It is important that the same Authorising Officer considers each authorisation to ensure that operational conflict and risks do not develop and to monitor the security and welfare of the CHIS. When appropriate, reviews should be combined to establish whether separate authorisations can be combined into a single authorisation to reduce bureaucracy and error.

Covert Surveillance of Social Networking Sites (SNS)

289. The fact that digital investigation is routine or easy to conduct does not reduce the need for authorisation. Care must be taken to understand how the SNS being used works. Authorising Officers must not be tempted to assume that one service provider is the same as another or that the services provided by a single provider are the same.

289.1 Whilst it is the responsibility of an individual to set privacy settings to protect unsolicited access to private information, and even though data may be deemed published and no longer under the control of the author, it is unwise to regard it as “open source” or publicly available, the author has a reasonable expectation of privacy if access controls are applied. In some cases data may be deemed private communication still in transmission (instant messages for example). Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required. Repeat viewing of “open source” sites may constitute directed surveillance on a case by case basis and this should be borne in mind.

289.2 Providing there is no warrant authorising interception in accordance with section 48(4) of the 2000 Act, if it is necessary and proportionate for a public authority to breach covertly access controls, the minimum requirement is an authorisation for directed surveillance. An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by a member of a public authority or by a person acting on its behalf (i.e. the activity is more than mere reading of the site’s content).

289.3 It is not unlawful for a member of a public authority to set up a false identity but it is inadvisable for a member of a public authority to do so for a covert purpose without an authorisation for directed surveillance when private information is likely to be obtained. The Senior Responsible Officer (SRO) should be satisfied that there is a process in place to ensure compliance with the legislation. Using photographs of other persons without their permission to support the false identity infringes other laws.

289.4 A member of a public authority should not adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without authorisation, and without the consent of the person whose identity is used, and without considering the protection of that person. The consent must be explicit (i.e. the person from whom consent is sought must agree (preferably in writing) what is and is not to be done).

Southend-on-Sea Borough Council

Agenda
Item No.
6

Report of Executive Director (Legal & Democratic Services)
to
Audit Committee
on
23 October 2019

Report prepared by: Tim MacGregor –Policy Manager

A Simple and Effective Governance Framework

Executive Councillor – Councillor Gilbert

A Part 1 Public Agenda Item

1. Purpose of Report

- 1.1 To review the Council's Local Code of Governance (now to be called 'A simple and effective governance framework').

2. Recommendations

- 2.1 **To recommend to Cabinet that they approve the revised Local Code of Governance – A simple and effective governance framework – as set out at Appendix A.**
- 2.2 **Once approved, that the Council's Constitution is updated to reflect the revised framework.**

3. Background

- 3.1 The Council is required to have in place a Local Code of Governance that sets out its governance framework. The framework outlines the Council's approach to good governance and enables the annual review of the effectiveness of internal control to be carried out. This review, a legal requirement, is undertaken via the Annual Governance Statement presented to Audit Committee each year, signed by the Leader and Chief Executive, and is published as part of the annual statement of accounts.
- 3.2 The 1992 Cadbury Committee report, set out recommendations on the arrangement of company boards and accounting systems to mitigate corporate risk and failures and defined corporate governance as the 'system by which organisations are directed and controlled'. Many of these recommendations were adopted by public sector bodies and complemented by the development of the Committee on Standards in Public life 'Nolan principles' to promote ethical standards across the whole of public life in the UK.

- 3.3 A good governance framework for local government was developed by the Chartered Institute of Public Finance and Accountancy (CIPFA) and the Society of Local Authority Chief Executives (SOLACE) and provides an over-arching framework to local authority local codes of governance. The framework has been revised a number of times, most recently in 2016, and the Council adopted the framework's seven core principles as the basis on which to operate.
- 3.4 In summary, the framework states that 'the overall aim is to ensure that resources are directed in accordance with agreed policy and according to priorities, that there is sound and inclusive decision making and that there is clear accountability for the use of those resources in order to achieve desired outcomes for service users and communities.'
- 3.5 It is part of the Council's Control Environment Assurance, which also includes the:
- risk management strategy
 - counter fraud, bribery and corruption policy and strategy
 - counter money laundering policy and strategy
 - whistleblowing policy
 - directed surveillance procedures.

4. A Simple and Effective Governance Framework - 2019

- 4.1 The current Local Code of Governance (agreed in 2016) has, therefore, been revised to reflect the direction of the council in recent years. This includes the adoption of the Southend 2050 Road Map, the council's new values and behaviours and changes to officer governance arrangements. It has also been simplified to remove (but provide links to) the CIPFA / SOLACE sub-principles of good governance and the Nolan principles of public life, but otherwise retains the core content of the 2016 Local Code of Governance.
- 4.2 The revised framework covers the following areas:
- What governance is;
 - The principles, values and behaviours to be adopted, setting the tone for how the organisation operates but also how councillors and officers conduct themselves;
 - The business management processes the Council operates to enable it to successfully deliver desired outcomes;
 - How the principles, values, behaviours and business management arrangements should be implemented;
 - The arrangements to complete the annual review of their adequacy and operation throughout the year, used to support the production of the Annual Governance Statement;
 - Evidencing effective implementation.
- 4.3 It will be necessary to ensure that Internal Audit's Strategy and Audit Plan, the Audit Committee's terms of reference and work programme and the Annual Governance Statement are consistent with the framework.

5. Other Options

- 5.1 Not adopting a revised simple and effective governance framework that incorporates would mean the Council's governance framework would lack clarity and would hinder delivery of the Southend 2050 outcomes.

6. Corporate Implications

6.1 Contribution to the Southend 2050 Road Map

Simple and effective governance is one of the seven transforming together 'conditions', identified as required for the delivery of the Southend 2050 ambition and desired outcomes for 2023.

6.2 Financial Implications - None specific

6.3 Legal Implications

Accounts and Audit (England) Regulations 2015, Section 4 requires that the relevant body must conduct a review at least once in a year of the effectiveness of its system of internal control.

The findings of the review must be considered by Council or by a committee. Following the review, the body or committee must approve an annual governance statement prepared in accordance with proper practices in relation to internal control.

Proper practice in this sense is defined as guidance issued by the relevant professional body, which for local government is the CIPFA / SOLACE Framework (refer background papers). This requires local authorities to produce a Local Code of Governance and sets out the operational framework that it should adopt.

Therefore compliance with this Code satisfies the requirements of the Accounts and Audit (England) Regulations 2015.

6.4 People Implications

All members and staff need to adopt the principles and the values and behaviours outlined in the framework and apply the business management processes required within their service areas.

6.5 Property Implications – None

6.6 Consultation

The relevant stakeholders have been consulted.

6.7 Equalities and Diversity Implications

This is reflected in both the principles, values and business management processes to be adopted.

6.8 Risk Assessment

Failure to operate robust governance arrangements can potentially lead to poor management, performance, stewardship of public money, public engagement and ultimately, poor outcomes for citizens and service users. It increases the risk that corporate priorities will not be delivered.

6.9 Value for Money

This is reflected in both the principles, values and business management processes to be adopted.

6.10 Community Safety Implications - None

6.11 Environmental Impact – None

7. Background Papers

- Chartered Institute of Public Finance and Accountancy (CIPFA) / Society of Local Authority Chief Executives and Senior Managers (SOLACE) publication: Delivering Good Governance in Local Government – Framework (2016).
- Chartered Institute of Public Finance and Accountancy (CIPFA) / Society of Local Authority Chief Executives and Senior Managers (SOLACE) publication: Guidance Note for English Authorities
- The Accounts and Audit (England) Regulations 2015

8. Appendices

Appendix 1 – A simple and effective governance framework – Southend on Sea Borough Council's Local Code of Governance

A simple and effective governance framework

Southend-on-Sea Borough Council's Local
Code of Governance (Draft)



Produced:
Next Review:
Time table for approval:

Tim MacGregor – Policy Manager
2022
Good Governance Group – 22.8.19
Corporate Management Team – 25.9.19
Audit Committee – 23.10.19
Cabinet – 5.11.19

1. What is governance and good governance?

Governance is defined by CIPFA and SOLACE as 'the arrangements put in place to ensure that the intended outcomes for stakeholders are defined and achieved'. Good governance helps deliver the outcomes desired by an organisation.

The Delivering Good Governance in Local Government Framework, published by CIPFA in association with SOLACE, sets the standard for local authority governance in the UK¹. It does so by stating that: 'To deliver good governance in the public sector, both governing bodies and individuals working for public sector entities must try to achieve their entities objectives while acting in the public interest at all times. Acting in the public interest implies primary consideration of the benefits for society, which should result in positive outcomes for service users and other stakeholders'.

All councils should aim to meet the standards of the best which means governance arrangements should not only be sound but also be seen to be sound. Achieving high standards of governance encourages others to have confidence in engaging with the Council, enabling it to be more effective in undertaking its role of community leader.

2. Purpose of the framework

This framework, adopted by the Council, is in line with good practice guidance, including the principles that underpin it. It is part of the Council's control environment assurance arrangements (outlined further in section 11).

The Council is accountable for the proper conduct of public business. This means ensuring it operates in accordance with the law and proper standards, and that public money is safeguarded, properly accounted for and used economically, efficiently and effectively. In doing this, the governance framework brings together an underlying set of values, legislative requirements, governance principles and management processes that enables effective outcomes.

The framework should be proportionate to the risk environment. As such one of the seven conditions the Council has established as required to achieve its [ambition](#) and desired outcomes is 'simple and effective governance'.

The underlying principles should be considered in the light of the key roles for local authorities identified in the guidance:

¹ [Delivering Good Governance in Local Government: Framework \(2016\)](#) Chartered Institute of Public Finance and Accountancy & Society of Local Authority Chief Executives and Senior Managers

1. To engage in effective partnerships and provide leadership for and with the community;
2. To ensure the delivery of high quality local services whether directly or in partnership or by commissioning;
3. To perform a stewardship role which protects the interests of local people and makes the best use of resources; and
4. To develop citizenship and local democracy.

The framework puts high standards of conduct and leadership at the heart of good governance, placing responsibility on councillors and officers to demonstrate leadership by behaving in ways that exemplify high standards of conduct and so set the tone for the rest of the organisation. The Council discharges accountability for the proper conduct of public business, through the publication of an Annual Governance Statement (AGS) that will make the adopted practice open and explicit.

This AGS also sets out:

- **Accountability** for the governance of the Council, as well as the principles and values by which the Council operates;
- How the **principles** are put into practice to enable service delivery to reflect community need and how evidence is obtained to ensure they operate effectively throughout the year;
- The annual **reporting** process and
- How the framework is **communicated** to councillors, staff and other relevant parties.

3. Accountability

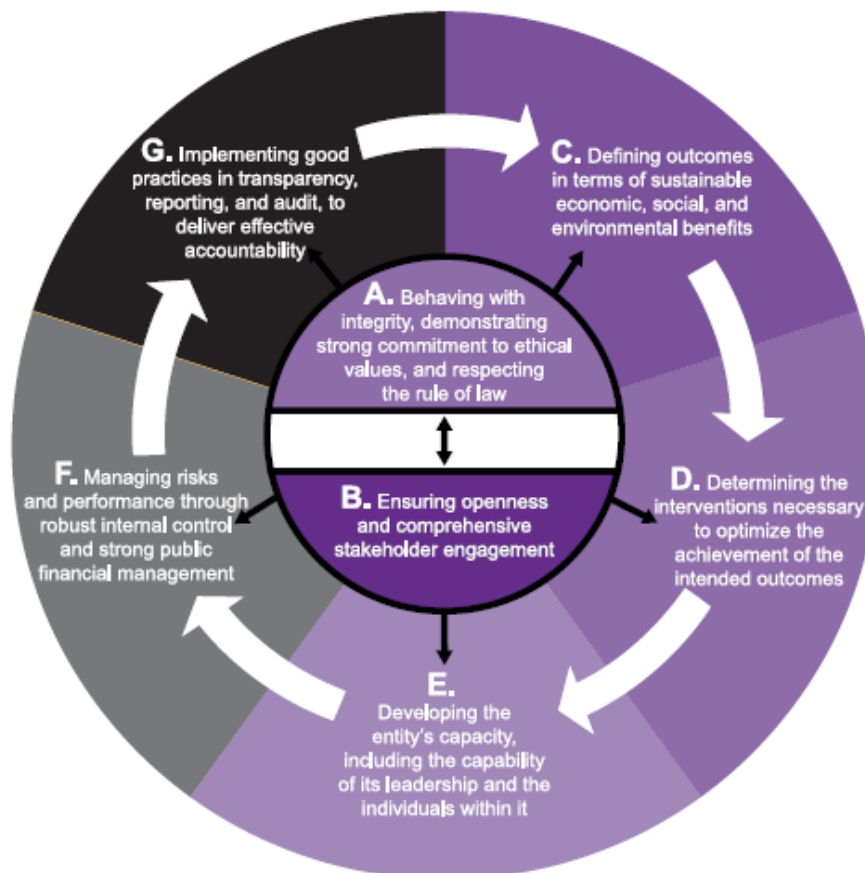
Councillors are collectively responsible for the governance of the Council. Council delegates responsibility for independently checking that an effective governance framework (which includes a sound system of internal control) exists and operates effectively throughout the year, to the Audit Committee.

The Leader of the Council and Chief Executive:

- Are accountable for ensuring good governance in their authority
- Sign the Annual Governance Statement on behalf of the Council.

4. Principles

The Council has adopted the seven core principles from the 2016 [CIPFA/Solace Framework](#) as the basis on which it wants to operate as outlined below.



The CIPFA/Solace governance framework provides more detail on how these core principles should be applied in practice. It provides context, along with the Nolan Principles of Public Life, for the Council's own values and behaviours, agreed in 2019. The adoption and implementation of these values and behaviours by staff and councillors is critical for Council to achieve its ambition and desired outcomes - as set out in the Southend 2050 Road Map.

5. Values and behaviours

In discharging their roles and implementing the principles outlined above at an individual level, councillors and staff are expected to adopt and enact;

- [The Nolan seven principles of public life](#)
- The Council's own values and behaviours:

Council values:

- **Inclusive – we put people at the heart of what we do**
- **Collaborative – we work together**
- **Honest – we are honest, fair and accountable**
- **Proud – we are proud to make lives better**

Behaviours expected of councillors and staff:

- **Driving positive change**
- **Trust and respect**
- **Demonstrating strong leadership**
- **Act with integrity and behaving responsibly**
- **Building relationships to work well together**

Adhering to these values and behaviours will help ensure that councillors and staff conduct complies with the overarching good governance principles.

6. Putting the principles into practice

All organisations, whether public or private, large or small, need to operate core management processes to enable them to deliver their vision, aims and objectives. These processes are outlined below under the Council's main management activities below:

| | |
|--|--|
| CITIZENS <ul style="list-style-type: none">• Community participation• Co-design and production with citizens• Customer satisfaction• Consultation and engagement• Complaints, compliments and comments | PERFORMANCE <ul style="list-style-type: none">• Outcome based business planning and strategy• Decision making / constitution• Policy framework and procedures• Performance management• Data quality• Risk management, whistleblowing• Business continuity• Information management security• Contract management• Project management• Change / transformation management |
| RESOURCES <ul style="list-style-type: none">• Outcome based financial planning & reporting, budgetary control and treasury management• Commissioning• Procurement• Asset Management• Fraud & Corruption and Insurance• Value for Money | PEOPLE <ul style="list-style-type: none">• Workforce management & development• Values and behaviours - codes of conduct for members and staff• Staff performance management• Health and safety• Ethical governance |

The Council also has a very specific responsibility for ensuring that:

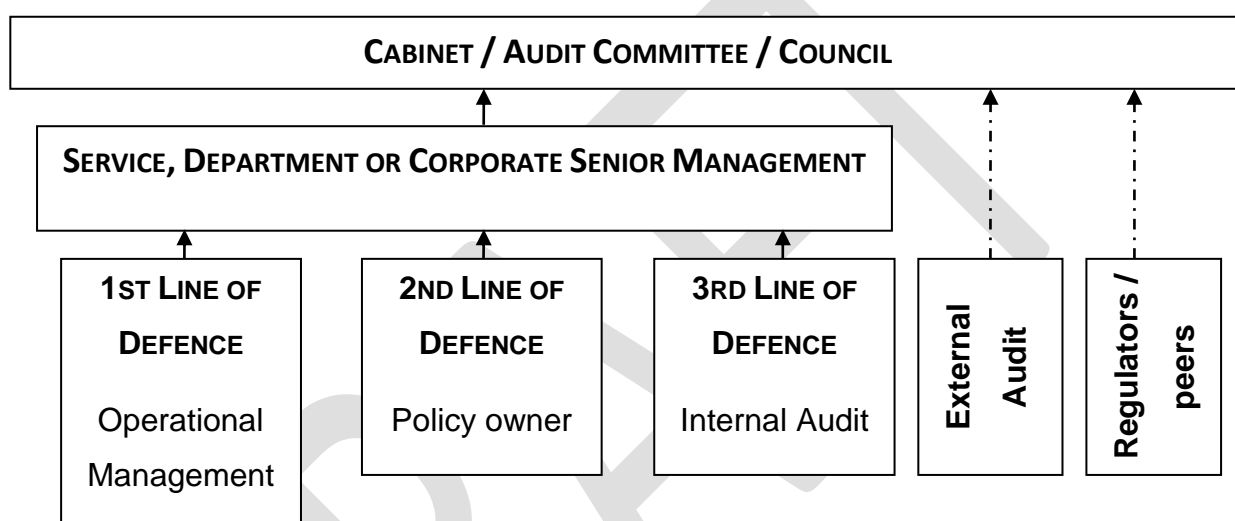
- The financial management of the body is adequate
- It has a sound system of internal control which facilitates the effective exercise of its functions and which includes its arrangements for the management of risk.

All services are responsible for maintaining proportionate but sound operational procedures and processes that adequately mitigate risks that may result in a service failure or the failure to deliver service objectives. Application of the framework outlined should put the Council in a strong position to successfully deliver whatever services it chooses to.

7. Effective implementation

7.1 The approach

In order to ensure that the governance framework set out above is in place and operating properly throughout the year, the Council has adopted the concept contained in the **three lines of defence**² model, as shown below.



Evidence that the governance framework is being applied is obtained via:

7.2 The first line of defence:

Operational management, which is responsible for the effective and consistent application of these requirements in their area of operation. This includes both behavioural as well as procedural arrangements.

7.3 The second line of defence:

The 'owner' or 'sponsor' who is accountable for the overall operation of the corporate management or service specific process and should ensure that:

- It is fit for purpose (for example, based upon relevant good practice), regularly reviewed and approved by senior management and members;

² Based upon general industry good practice, more specifically guidance issued by the European Confederation of Institutes of Internal Auditing "*monitoring the effectiveness of internal control, internal audits and risk management systems*" September 2010

- It is constructed so that evidence of its application is easily produced, i.e., as 'business as usual';
- There are proportionate and cost-effective mechanisms in place to enable them to confirm that operational managers are applying it effectively and consistently; and
- Informative, regular and timely reports are provided to senior management to confirm the process has been operating effectively and consistently, identifying any remedial actions required should this not be the case.

7.4 The third line of defence which is:

Internal Audit who provide **independent assurance** to senior management and the Audit Committee, on how effectively the first and second lines of defence have been operating.

7.5 System of Internal Control

Within this, it is incumbent on all staff to ensure that:

- sufficient checks (controls) are built into all systems, processes and activities to ensure that they consistently and effectively deliver the objectives required of them (e.g. through risk management / mitigation);
- sufficient evidence can be obtained throughout the year (via key management controls) to ensure these checks are operating as they should and, therefore, that the systems, processes and service objectives are being delivered.

7.6 Other potential assurance

This can be obtained from external sources such as external audit, regulators, peers as well as the public and media and can be considered a **fourth line of defence** where any of these sources' activity is relevant and robust.

8. Key Committees

The ('full') Council is responsible for ensuring the organisation has good governance arrangements. It can discharge this duty itself or delegate this role to a committee.

The Council has delegated this function to the Audit Committee. However, there are other key council bodies that have a significant role to play within the governance framework:

- Full Council is responsible for setting the budget and policy framework.
- The **Cabinet** is responsible for the majority of functions of the Council. Executive decisions are taken by the Cabinet collectively or by officers acting under delegated powers. Cabinet leads the Council's drive for value for money, the preparation of the Council's vision, policies and budget and community participation processes. It takes in year decisions on resources and priorities and is the focus for forming partnerships to address local needs.
- **Scrutiny Committees** review decisions made or actions taken in relation to any of the Council's functions, consider any matter affecting the area or its residents and exercise the right to call in, for reconsideration, decisions made by Cabinet, not yet implemented. They undertake reviews of Council policy and practice and suggest ways these could be improved.
- **Audit Committee** is responsible for independently checking that appropriate governance arrangements (including the system of internal control) are in place, operating effectively throughout the year and that actions required to strengthen these arrangements are addressed, in a timely manner. Its work programme is designed to provide it with sufficient evidence to conclude that the Annual Governance Statement accurately reflects the governance arrangements as operated for the year in question.
- The **Standards Committee** is responsible for promoting and maintaining high standards of conduct by councillors and co-opted members, and assisting them to observe the Councillors code of conduct.
- The **Health & Wellbeing Board** provides strategic leadership to improve the health and wellbeing of local people and reduce health inequalities. The Board works to understand the local community's needs, agree priorities and encourage commissioners to work in a more joined up way.
- The **Community Safety Partnership** provides strategic leadership in their statutory responsibility for reducing crime and disorder, substance misuse and re-offending in their area.

It is necessary sometimes for information to go to more than one committee in order for them to discharge their respective responsibilities.

9. Good Governance Group

The Council has an officer Good Governance Group that meets regularly to oversee the delivery of the governance framework. There is a terms of reference for this group and it reports to the Chief Executive and provides reports to the Corporate Management Team and Audit Committee.

In addition to the Corporate Management Team, key officer boards ensure good governance in relation to:

- Investment
- Commissioning
- Growth & infrastructure
- Innovation and change

10. Annual review and reporting

Local authorities are required to undertake an annual review their governance arrangements and evidence that they are:

- Up to date, fit for purpose and comply with the CIPFA/Solace Framework;
- Consistently applied across the organisation at all service levels;
- Being strengthened, as necessary, where improvement opportunities have been identified.

Such reviews are reported to the Audit Committee, within the Council and externally with the published accounts.

11. Evidence and Assurance

Evidence that the governance framework is operating as it should, is obtained in a number of ways. This includes:

Annual assurance obtained from:

- Key elements of the Control Environment Assurance, including the Council's approach to and reporting on:
 - Risk management
 - Counter fraud, bribery and corruption
 - Counter money laundering
 - Whistleblowing
 - Directed surveillance

The owners or sponsors of key management processes, in relation to the adequacy of and compliance with key management arrangements

- Other significant functions / service providers (e.g. project / contract managers) that confirms compliance with the relevant corporate approach or requirements.
- The Good Governance Group reviewing evidence provided, each year, highlighting any areas that require senior management attention. Departmental management teams will review actions requiring attention through the normal performance management process.
- Compliance with the treasury management policy.
- Approval of the financial statements.
- Revenue and capital monitoring.
- Performance management.

12. Independent evidence

Independent evidence primarily takes the form of:

- The Head of Internal Audit's annual report, which includes an opinion on the overall system of internal control and whether the internal audit functions have complied with professional standards.
- The external auditor's Annual Governance Report to those charged with governance.
- External inspections and reviews from regulatory, professional, peer and representative bodies.

13. Annual Governance Statement

The Council's Annual Governance Statement is developed by the Good Governance Group, during the year and will be considered by the Corporate Management Team before being reported to the Audit Committee as part of the annual Statement of Accounts. The Audit Committee considers whether the Annual Governance Statement accurately reflects its understanding of how the Council's governance arrangements have operated for the year in question.

The AGS is signed by the Leader and Chief Executive on behalf of the Council.

14. Communications

This framework forms part of the Council's Constitution which is available on Council's website and, therefore, accessible to all staff, councillors, the public and other stakeholders. The framework is provided to new councillors and content outlined to newly appointed staff as part of the induction process.

Training on aspects of the governance framework or the application of key business management processes is provided as required.

The Head of Internal Audit can be contacted on 01702 215802 and the Policy Manager can be contacted on 01702 534025 with any queries regarding the framework.

This page is intentionally left blank

Southend-on-Sea Borough Council

Agenda
Item No.

7

Report of the Chief Executive

to

Audit Committee

on

23rd October 2019

Report prepared by: Andrew Barnes, Head of Internal Audit

Internal Audit Services, Quarterly Performance Report

A Part 1 Public Agenda Item

1. Purpose of Report

- 1.1 To update the Audit Committee on the progress made in delivering the Internal Audit Strategy and Plan for 2019/20.

2. Recommendations

- 2.1 **The Audit Committee notes the progress made in delivering the 2019/20 Internal Audit Strategy.**

3. Internal Audit Plan Status

- 3.1 **Appendix 1** sets out the current status of the audit work planned for the year as at 11th October 2019. This highlights where audits contained in the original plan considered by the Audit Committee in March 2019 have changed and why. This includes adding audits to the plan from the Risk Watch list, as we have increased the team's capacity by recruiting more in-house audit staff, reducing the need to use the framework contract to resource audits, and additional Advice and Support work that we have been asked to contribute to.
- 3.2 **Appendix 2** sets out the results of the work completed since the last progress report to the Audit Committee in July.

4. Performance Targets

- 4.1 As outlined in the Strategy presented to the March 2019 Audit Committee, the team will be reporting on a more limited set of indicators this year given the amount of work that is still being contracted out.

4.2 So as at 11th October 2019:

- the team has had 4.5 of sickness absence since 1st April 2019 (which impacts on productivity) and equates to 0.76 days per FTE
- in terms of the jobs in the plan:
 - 14% of audits are completed
 - 2% of audits have reports being produced or discussed
 - 13% of audits are in progress
 - 14% of audits are being scoped and planned or have terms of reference produced
 - 53% of audits are resourced and booked, but yet to be started
 - 4% of audits have resourcing being finalised

4.3 A programme of stakeholder surveys has been produced and these will be completed throughout the remainder of the year as audits are completed.

Appendix 3 reflects the results of 7 surveys covering 6 audits undertaken since the last meeting. Overall the feedback obtained remains very positive. The key overall message is that stakeholders find the Council's Internal Audit service to be professional, approachable, flexible and of tangible benefit to their services as well as the Council as a whole.

4.4 In addition it is worth noting some very positive feedback that was provided in respect of one complicated area that we have audited. The respondent provided a range of positive feedback and concluded that 'I welcome internal audits. It gives a fresh pair of eyes and provides challenge in a constructive way. I have always learnt so much by going through the process.' which is very much what we are trying to deliver as a team.

5. Resourcing

5.1 Since the last report to the Audit Committee in May 2019:

- a Senior Auditor has been promoted to Audit Manager
- an Auditor joined the team in September
- a Senior Auditor has been appointed and is due to join the team in October.

5.2 That leaves the combined team with four vacancies. The salaries of the vacant posts are currently being used to fund audit resource brought in from suitable accountancy firms to assist with delivery of the audit plan. Time is also being spent supporting the development of in-house staff, with action plans in place to support and monitor the progress of their development, to enhance the effectiveness of the team overall.

5.3 The expected requirements of the internal audit service into the future continue to evolve and this has been assessed to determine the most appropriate team model utilising the financial resources available. Once the current team resourcing activities are complete, this will then be implemented to result in an appropriate mix of experienced staff, trainees who will be put through a relevant training programme and externally sourced skills. This will enable the team to deliver the internal audit service required by the organisations that it serves.

6. Corporate Implications

6.1 Contribution to Council's Aims and Priorities

Audit work contributes to the delivery of all corporate Aims and Priorities.

6.2 Financial Implications

The Audit Plan will be delivered within the approved budget.

Any financial implications arising from identifying and managing fraud risk will be considered through the normal financial management processes.

6.3 Legal Implications

The UK Public Sector Internal Audit Standards require the Audit Committee to approve (but not direct) the annual Internal Audit Plan and then receive regular updates on its delivery. This report contributes to discharging this duty.

6.4 People and Property Implications

People and property issues that are relevant to an audit within the Audit Plan will be considered as part of the review.

6.5 Consultation

The audit risk assessment and the Audit Plan are periodically discussed with the Chief Executive, Deputy Chief Executives and Directors before being reported to Corporate Management Team and the Audit Committee.

All terms of reference and draft reports are discussed with the relevant Deputy Chief Executives and Directors before being finalised.

6.6 Equalities Impact Assessment

The relevance of equality and diversity is considered during the initial planning stage of the each audit before the Terms of Reference are agreed.

6.7 Risk Assessment

Failure to operate a robust assurance process (which incorporates the internal audit function) increases the risk that there are inadequacies in the internal control framework that may impact of the Council's ability to deliver its corporate aims and priorities.

The main risks the team continues to manage are the:

- potential loss of in-house staff and the ability of the service to replace this resource in a timely manner
- lack of management capacity to support and process work in a timely manner and provide strategic leadership to the team
- possibility that the external supplier won't deliver contracted in work within the required deadlines to the expected quality standards
- need to maintain relationships with clients / partners until the service has been rebuilt.

6.8 Value for Money

Opportunities to improve value for money in the delivery of services are identified during some reviews and recommendations made as appropriate.

Internal Audit also considers whether it provides a value for money service periodically.

6.9 Community Safety Implications and Environmental Impact

These issues are only considered if relevant to a specific audit review.

7. Background Papers

- The Accounts and Audit Regulations 2015
- UK Public Sector Internal Audit Standards
- CIPFA: Local Government Application Note for the UK Public Sector Internal Audit Standards

8. Appendices

| | |
|-------------|--|
| Appendix 1 | Internal Audit Plan 2019/20 |
| Appendix 2A | Assurance summary: satisfactory assurance |
| Appendix 2B | Assurance summary: partial assurance |
| Appendix 2C | Assurance summary: other audits and grants |
| Appendix 2D | Assurance summary: follow up audits |
| Appendix 3 | Stakeholder survey results |

Appendix 1: Internal Audit Plan 2019/20

| Dept & (Lead) | Service Activity | Fraud risk | Status at October 2019 |
|----------------------------------|--|------------|---|
| Managing the Business | | | |
| All Outcomes | | | |
| All | Risk Management Strategy To lead on the Council's work to embed a robust and efficient risk management framework into its wider governance arrangements. | No | Risk Management Policy Statement and Strategy agreed by Cabinet September 2019. Agreed Implementation Action Plan to test and roll out the new approach between September 2019 to May 2020. (See also IT Risk Assessment and Better Queensway below) |
| PL (ST) | IT Risk Assessment To undertake a baseline assessment of IT risks against a standard good practice framework and use this to develop the IT element of the Audit Plan going forward. | No | Focus will be informed by the IT risk workshop taking place with the service on 23 October 2019. |
| Implementing Action Plans | | | |
| F&R (JC) | Shareholder Board To check that actions agreed have been effectively implemented and are now embedded into the day to day operation of the service. | No | All planned for January to March 2020. |
| L&D (JW) | Emergency Planning To check that actions agreed have been effectively implemented and are now embedded into the day to day operation of the service. | No | |
| L&D (JW) | Business Continuity To check that actions agreed have been effectively implemented and are now embedded into the day to day operation of the service. | No | |

Appendix 1: Internal Audit Plan 2019/20

| Dept & (Lead) | Service Activity | Fraud risk | Status at October 2019 |
|--|--|------------|------------------------------------|
| T (JR) | Information Governance, General Data Protection Regulations To check that actions agreed have been effectively implemented and are now embedded into the day to day operation of the service. | No | Planned for January to March 2020. |
| Managing Service Delivery Risks | | | |
| Pride and Joy By 2050 Southenders are fiercely proud of and go out of their way to champion what our city has to offer. | | | |
| PL (NH) | Local Transport Capital Block Funding - Flood Resilience To certify, in all significant respects, that the conditions attached to the grant have been complied with. | Yes | Completed September 2019. |
| PL (NH) | National Productivity Investment Fund – Town Centre Redevelopment Improvement Project To certify, in all significant respects, that the conditions attached to the grant have been complied with. | Yes | Completed September 2019. |
| Implementing Action Plans | | | |
| No work required | | | |
| Safe and Well By 2050 people in Southend-on-Sea feel safe in all aspects of their lives and are well enough to live fulfilling lives | | | |
| PE (BM) | Children Centres Contract Management (2018/19) To assess whether the contract is being effectively managed to ensure the planned outcomes for children and families are being delivered in compliance with the specified performance and/or quality standards, at the correct price. | No | Completed July 2019. |

Appendix 1: Internal Audit Plan 2019/20

| Dept & (Lead) | Service Activity | Fraud risk | Status at October 2019 |
|---------------|--|------------|---|
| PE (GH) | Homelessness and Rough Sleeping To assess the robustness of arrangements for quickly and effectively supporting people facing homelessness to prevent this from happening and where it does that this is brief and non-recurrent. | Yes | Work in progress. |
| PE (JOL) | Independent Reviewing Officers To assess the effectiveness of Independent Reviewing Officers in ensuring children's needs are met and their outcomes improved through the support and services that they receive, enabling them to reach their potential. | No | Work in progress. Internal Audit working with Children's Services to agree an overall action plan as the findings of an independent review also emerge. |
| PE (JL) | Commissioning of a New Service To assess whether commissioning decisions were evidence based through clear and concise commissioning proposals, in order to meet the needs and outcomes required. | Yes | Initial planning and scoping of the work underway. |
| PE (JL) | Outcome Realisation of a Commissioned Service To assess whether the delivery of a commissioned service is being effectively managed to ensure the planned outcomes and / or benefits for residents anticipated by the commissioning process are delivered. | Yes | Initial planning and scoping of the work underway. |
| PE (GH) | Private Sector Housing To assess the effectiveness of the Private Sector Housing offer in regeneration of the housing market to ensure inclusive, healthy and safe places to live. | Yes | Planned January to March 2020. |
| PE (JOL) | In House Foster Carers To assess the effectiveness of arrangements to recruit and retain in-house Foster Carers, including the ongoing training and support provided to them to ensure local, stable foster placements for children. | Yes | Planned October to December 2019. |

Appendix 1: Internal Audit Plan 2019/20

| Dept & (Lead) | Service Activity | Fraud risk | Status at October 2019 |
|------------------|---|------------|---|
| PL (CR) | Environmental Health To assess whether there are robust arrangements in place to ensure concerns and referrals received are properly and effectively dealt with and statutory responsibilities discharged to protect and improve the wellbeing of residents. | | New addition to the Audit Plan from the risk Watch list (see Appendix 2a) as in house resource increased. Initial planning and scoping of work underway. |
| PE (SB) | Deprivation of Liberty Safeguards (DoLS) To assess the robustness of arrangements which ensure when a person is deprived of liberty, is necessary and in their best interests. | | New addition to the Audit Plan from the risk Watch list (see Appendix 2a) as in house resource increased. Planned for January to March 2020. |
| PE (SB) | Adult Social Care Financial Assessments To assess the robustness of the process that determines eligibility for financial support towards care needs to ensure it is accurate, transparent and accessible. | Yes | Terms of reference prepared. |
| PE (MB / JOL) | Data Quality – Children’s Services To assess the robustness of arrangements to confirm that data entered into the care management system (LCS) by social care staff, which is then used to produce performance indicators for senior management, is reliable. | No | Terms of reference prepared. |
| PL (PG) | Building a Safer Future To assess the Building Control team’s preparedness for implementing the changes to Building Regulations and Fire Safety emanating from the Hackitt Enquiry published in December 2018. | No | Planned January to March 2020. |
| PE (JOL) | Early Help and Family Support Quality Assurance Framework To assess the effectiveness of the Assurance Framework in supporting the Edge of Care Team to ensure that the right decisions are made to meet children’s needs and keep them safe. | No | Planned October to December 2019. Under review as Children Services are considering the overall extent of the quality assurance framework. |

Appendix 1: Internal Audit Plan 2019/20

| Dept & (Lead) | Service Activity | Fraud risk | Status at October 2019 |
|---|---|------------|---|
| PE (GH) | Disabled Facilities Grant To certify that, in all significant respects, the conditions attached to the grant have been complied with. | Yes | Completed September 2019. |
| PE (JOL) | Troubled Families To certify that, in all significant respects, the conditions attached to the grant have been complied with. | Yes | Report on the July to September 2019 submissions completed September 2019. |
| Implementing Action Plans | | | |
| PL (PG) | Building Control To check that actions agreed have been effectively implemented and are now embedded into the day to day operation of the service. | Yes | Draft report being discussed with the client. |
| PE (JOL) | Management Response to Quality Assurance Audits (2018-19) To assess whether the actions agreed in the original audit dated July 2018 have been implemented and are now effectively embedded into the day-to-day operation of the service. | No | Completed October 2019. |
| PE (JOL) | Social Care Payments to Individuals and Providers – Children (2018-19) To assess the robustness of the arrangements identified in the previous memo issued in June 2018, in ensuring that accurate and timely social care payments are made to individuals and providers. | Yes | Completed October 2019. |
| <p style="text-align: center;">Active and Involved</p> <p style="text-align: center;">By 2050 we have a thriving, active and involved community that feel invested in our city</p> | | | |
| Implementing Action Plans | | | |
| PL (PG) | South Essex Active Travel (SEAT) Governance Arrangements To check that actions agreed have been effectively implemented and are now embedded into the day to day operation of the service. | Yes | Work in progress. |

Appendix 1: Internal Audit Plan 2019/20

| Dept & (Lead) | Service Activity | Fraud risk | Status at October 2019 |
|---|--|------------|---|
| Opportunity and Prosperity By 2050 Southend-on-Sea is a successful city and we share our prosperity amongst all of our people | | | |
| T (JR) | Hayes Contract Management To assess whether there are robust arrangements in place to ensure that the contract is delivering the planned outcomes and / or benefits in compliance with the specified performance and quality standards, at the correct cost. | Yes | Planned January to March 2020. |
| PL (PG) | Parking Enforcement Income Collection To assess the effectiveness of arrangements for the timely collection of this income in line with the expectations set out in the Corporate Debt Policy (November 2017). | Yes | Planned January to March 2020. |
| PL (PG) | Rechargeable Works To assess the effectiveness of arrangements for recharging third parties for the cost of making good accidental damage to Council assets. | Yes | Initial planning and scoping of the work underway. |
| Implementing Action Plans | | | |
| No work required | | | |
| Connected and Smart By 2050 people can easily get in, out and around our borough and we have a world class digital infrastructure | | | |
| PL (ST) | IT Audit – Focus TBD The focus of these audits will be determined following the IT Risk Assessment work starting in October 2019 (see Managing the Business above). | Yes | Timings to be determined after the IT Risk Assessment work above (Managing the Business). |
| PL (ST) | IT Audit – Focus TBD The focus of these audits will be determined following the IT Risk Assessment work starting in October 2019 (see Managing the Business above). | Yes | |

Appendix 1: Internal Audit Plan 2019/20

| Dept & (Lead) | Service Activity | Fraud risk | Status at October 2019 |
|----------------------------------|--|------------|---------------------------------------|
| PL (PG) | Local Transport Capital Block Funding - Highways Maintenance To certify that, in all significant respects, the conditions attached to the grant have been complied with. | Yes | Completed September 2019. |
| PL (PG) | Pothole Action Fund To certify that, in all significant respects, the conditions attached to the grant have been complied with. | Yes | Completed September 2019. |
| Implementing Action Plans | | | |
| No work required | | | |
| Key Financial Systems | | | |
| All Outcomes | | | |
| T (JR) | Payroll (2018/19) To assess the robustness of arrangements which ensure staff are paid the right amount at the right time in line with Council policies and legislative requirements. | Yes | Completed August 2019. |
| F&R (JC) | Housing Benefits To assess whether the key controls effectively prevent or detect material financial errors, on a timely basis, so that information from the system can be relied upon when producing the Council's statement of accounts. | Yes | Planned for October to December 2019. |
| F&R (JC) | Council Tax To assess whether the key controls effectively prevent or detect material financial errors, on a timely basis, so that information from the system can be relied upon when producing the Council's statement of accounts. | Yes | |
| F&R (JC) | Accounts Payable – Batch Input Files (BIF) To assess the robustness of arrangements to ensure that these payment files are accurate and secure. | Yes | Planned for January to March 2020. |

Appendix 1: Internal Audit Plan 2019/20

| Dept & (Lead) | Service Activity | Fraud risk | Status at October 2019 |
|----------------------------------|--|------------|--|
| F&R (JC) | Income Management System To assess the robustness of the new system to ensure that all income is accounted for in an accurate, secure and timely manner. | Yes | Finalising resource for this work. |
| PE (SB) | Social Care Debt Collection To assess the effectiveness of arrangements for the timely collection of this income in line with the expectations set out in the Corporate Debt Policy (November 2017). | Yes | Terms of reference being drawn up. |
| Implementing Action Plans | | | |
| T (JR) | Payroll To check that actions agreed have been effectively implemented and are now embedded into the day to day operation of the service. | Yes | New addition to the Audit Plan from the risk Watch list (see Appendix 2a) as in house resource increased. Planned January to March 2020. |
| Advice and Support | | | |
| All Outcomes | | | |
| PL (AL) | Cyber Security To provide support and challenge over the robustness of the arrangements for implementing the improvement actions identified by the Local Government Association's 'stock take' of resilience arrangements against cyber-attacks. | Yes | Timing to be aligned to the council's internal reporting arrangements. |
| All | Transforming Together & Southend 2050 To provide support and challenge to the organisation as these continue to develop. | No | No work this quarter. |
| All | Information Asset Register Group To provide support and challenge to the group as the Information Asset Register continues to develop. | No | No work this quarter. |

Appendix 1: Internal Audit Plan 2019/20

| Dept & (Lead) | Service Activity | Fraud risk | Status at October 2019 |
|--|---|------------|--|
| GGG ¹ | Subject Access Requests Children's Services To provide support and challenge around the robustness of arrangements for responding to these requests in the required time frames. (Working with the Transformation Service's Service Design Team) | No | New. Extent of the work and resourcing required being determined. |
| Pride and Joy By 2050 Southenders are fiercely proud of, and go out of their way, to champion what our city has to offer. | | | |
| No work planned. | | | |
| Safe and Well By 2050 people in Southend-on-Sea feel safe in all aspects of their lives and are well enough to live fulfilling lives | | | |
| PL (AL) | Fire Safety To provide support and challenge to the working group to ensure that fire safety arrangements are appropriate and effectively managed to make buildings safe and feel safe, now and in the future. | Yes | Work in progress. |
| Active and Involved By 2050 we have a thriving, active and involved community that feel invested in our city | | | |
| No work planned. | | | |

¹ Good Governance Group

Appendix 1: Internal Audit Plan 2019/20

| Dept & (Lead) | Service Activity | Fraud risk | Status at October 2019 |
|--|---|------------|--|
| <p align="center">Opportunity and Prosperity</p> <p align="center">By 2050 Southend-on-Sea is a successful city and we share our prosperity amongst all of our people</p> | | | |
| PL (EC) | <p>Better Queensway Joint Venture</p> <p>To provide support and challenge as the organisation develops and implements governance arrangements to monitor the delivery of the programme through the Joint Venture Limited Liability Partnership.</p> | Yes | Risk Workshop on 13 November 2019 to pilot new risk management arrangements (see Risk Management Strategy above under Managing the Business). |
| All | <p>Corporate Establishment</p> <p>To provide support and challenge over the development of a corporate establishment, with the purpose of ensuring a complete and accurate personnel establishment list within Agresso and realisation of associated benefits.</p> | Yes | Timing to be determined once the project timeline has been agreed. |
| PE / F&R (BM / JC) | <p>Use of the Basic Need Capital Grant for Schools</p> <p>To support the Council in determining its role and responsibilities in ensuring value for money for the provision of increased pupil places.</p> | Yes | Completed April 2019. |
| <p align="center">Connected and Smart</p> <p align="center">By 2050 people can easily get in, out and around our borough and we have a world class digital infrastructure</p> | | | |
| PL (PG) | <p>Highways Improvement Plan</p> <p>To provide support and challenge over the robustness of the arrangements for implementing the agreed improvement actions and for measuring the positive impact of the actions.</p> | No | Feedback provided covering the clarity of ownership and agreed target dates for actions detailed in the Improvement Plan. |

Appendix 1: Internal Audit Plan 2019/20

| Dept & (Lead) | Service Activity | Fraud risk | Status at October 2019 |
|---|------------------|------------|------------------------|
| Managing Service Delivery | | | |
| <p>Delivering the internal audit service involves:</p> <ul style="list-style-type: none"> • audit planning and resourcing • managing Audit Plan delivery which includes overseeing contractor work • reporting to senior management and the Audit Committee. | | | |
| <p>Implementing the outstanding actions arising from the external quality assessment undertaken by the Institute of Internal Auditors undertaken in October 2017.</p> | | | |

Appendix 2a: Internal Audit Plan 2019/20

| Risk Watch List | |
|-----------------|---|
| PE | The effectiveness of the Children's Services Quality Assurance and Practice Framework |
| PE | Adherence to terms and conditions of the Early Years grant funding (advice and support 2019/20) |
| PE | Delivery of outcomes from the block contract with Southend Care |
| PE | Monitoring the delivery of outcomes for older people placed in residential care |
| PE | Implementation of the Special Education Needs Inspection Action Plan |
| PE | Essex Partnership University NHS Foundation Trust S75 Agreement |
| F&R | Counter Fraud and Investigations delivery against the Service Level Agreement with Thurrock Council (New alternative arrangements now being developed) |
| PL | Management of the ICT Liquid Logic and / or Logicalis contract |
| PE | Delivery of outcomes from the Locality delivery model in Adult Social Care |
| PL | Environmental Health (Now added to the 2019/20 Audit Plan) |
| T | Payroll revisited (Now added to the 2019/20 Audit Plan) |
| PE | Vibrance contract management revisited |
| T | Governance architecture for service delivery |
| F&R | Implementation of the automated P2P new supplier process (advice and support 2019/20) |
| PE | Deprivation of Liberty Safeguards (DoLS) (Now added to the 2019/20 Audit Plan) |

These are other potential audits that may be considered for inclusion in the Audit Plan during the year should resources permit.

Appendix 2a: Internal Audit Plan 2019/20

| Audit Activities | Resource allocation |
|--------------------------------------|----------------------------|
| Managing the Business | 3% |
| Managing Service Delivery Risks | 42% |
| Key Financial Systems | 13% |
| Grant Claims | 6% |
| Advice and Support | 7% |
| Follow Ups | 8% |
| Contingency | 11% |
| Managing Delivery of the Audit Plan | 10% |
| Total | 100% |
| | |
| Total Council Audit Plan Days | 583 |
| | |

The days required to revisit and retest action plans from previous reports are included under each heading.

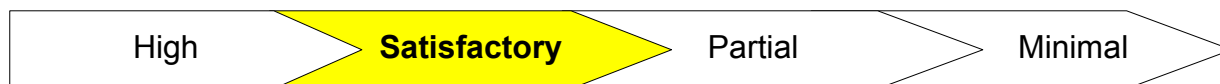
The Total Council Audit Plan Days reflects the higher cost of buying in external contractors to cover internal vacancies.

| Analysis Over Departments | | |
|----------------------------------|-------------------------------------|-------------|
| All | Cross Cutting | 4% |
| F&R | Finance and Resources Service | 11% |
| L&D | Legal and Democratic Services | 3% |
| T | Transformation Service | 4% |
| PE | People | 32% |
| PL | Place | 25% |
| All | Contingency | 11% |
| All | Managing Delivery of the Audit Plan | 10% |
| | Total | 100% |

This page is intentionally left blank

Appendix 2A: Assurance and Themes

Assurance



Contract Management of Children's Centres (2018/19)

Objective

To assess whether the contract is being effectively managed to ensure the planned outcomes for children and families are being delivered in compliance with the specified performance and / or quality standards, at the correct price

Themes

The contract for management of the Children's Centres commenced on 1 October 2016. From the outset, the Council recognised that the service provider's ability to achieve the Key Performance Indicators within the contract was affected by a requirement to TUPE existing staff and restructure the service, while containing the costs within the Council's maximum budget envelope. It was also affected by a number of the Key Performance Indicators (KPIs), which required partnership working with other organisations.

To address this, the Council proposed changes to the contract that led to a formal Contract Variation during April 2018. The variation changed the KPIs reducing their number and classifying them across three themes Access to Services, Quality of Services and Partnership Working.

This classification recognised that the service provider is largely an enabler of opportunity in capturing families and children into a wider partnership system of working with people/other agencies to improve outcomes.

Since April 2018, the council has put in place two Action Plans to respond to concerns over delivery of the KPIs. The first concentrates on the number of children living in deprivation areas who are attending a children's centre, and the second on maximising the use of the buildings. The second action plan recognises that many of the KPIs cannot be delivered to their maximum potential without the Children's Centres being opened and occupied in pursuit of meaningful activity related to delivering them. It is reported that there is currently a particular focus on three children centres through 'test and learn' initiatives with partners, to start the change to improve service delivery and outcomes.

Since April 2018, progress on meeting the actions has been robustly managed and monitored at a senior level by the Director of Learning in accordance with recommended practices, to maximise what can be achieved. The contract is also monitored by the Success For All Group and the Department for People's Major Projects Group.

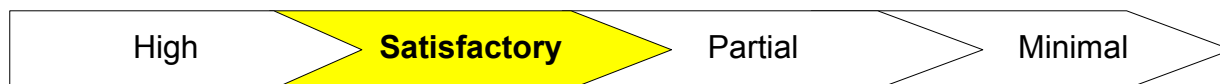
The Deputy Chief Executive (People) has authorised additional expenditure up to the Council's original budget envelope to mitigate the early effect of a reduced service, as resources were consumed in restructuring costs.

Contractual payments to date have been held within the budget envelope.

Going forward there is recognition that as the delivery of this service approaches the end of the current contractual arrangement, there will be significant opportunities to re-examine how outcomes can best be achieved by applying the principles laid out in

Appendix 2A: Assurance and Themes

Assurance



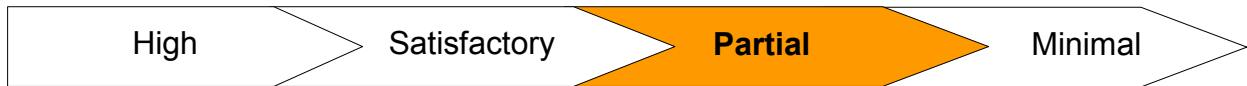
the council's Commissioning Framework. There is a particular acknowledgement that effective commissioning requires collaboration with partners and other key Stakeholders.

Better defining realistic outcomes and associated performance measures for children and families will ensure the contractual behaviour drives performance for contracted services, if that is the service delivery model selected, necessary to achieve the council's 2050 ambition and five-year road map.

Number of actions agreed: 3

Appendix 2B: Audit Assurances and Themes

Assurance



Payroll

Objective

To assess the robustness of arrangements which ensure staff are paid the correct amount at the right time in line with Southend on Sea Borough Council's (the Council) policies and legislative requirements.

Summary

Annual uplifts of salary scales, tax codes and national insurance bands within Business World are timely, with two officers involved in each process to ensure they are accurate. Business World permissions are reviewed on an annual basis to ensure access to Payroll and HR functions are appropriately restricted.

The payroll processing guide provides direction to staff on running reports ahead of the payroll being processed. Work is underway to extend the guidance to ensure all processes are covered and to ensure expectations of the checks needed are clear.

The process for inputting pay forms (for starters, leavers and amendments), overtime outside of self-serve, allowances and additional run payments onto Business World is manual and requires:

- one officer signing the supporting evidence to confirm they have input the information onto Business World
- a second officer independently reviewing the input and signing the supporting evidence to confirm it is accurate.

A number of instances were identified where the input had not been reviewed by the second Officer. Extending the monthly spot check of pay forms currently undertaken to include a selection of the manually input overtime, allowances and additional run transactions will help to:

- ensure they are processed correctly and supported by appropriate evidence
- identify those that have not followed the correct review and authorisation process
- deter inappropriate payments being input on the system.

Once the payroll is prepared and in proposal, a deviance report is run to identify all individual payments that are +/- 30% or more compared to the previous month. Spot-checking those below the 30% threshold will help deter fraudulent payments made in a way to circumvent this check. As it is not possible to physically stop changes to the payroll while it is being processed, a second deviance report is run to identify any additional transactions during 'lockdown'. This check is being extended to confirm the value of payments is also unchanged.

Two Officers are involved in uploading the payment file for the BACS run. They check the file to ensure the value is as expected and therefore that payment is correct.

Appendix 2B: Audit Assurances and Themes

Assurance



After the payroll has been run, a 'net pay' check compares the second deviance report to actual pay to confirm no further changes were made.

A long term, wider piece of work is underway to build an 'establishment hierarchy' into Business World, enabling employees to be allocated to posts within the set organisational structure. This should:

- ensure an accurate record of staff is maintained and give greater control over staff resources and appropriateness of payments
- allow for a more automated payroll process, especially for input and review of information into Business World.

Number of actions agreed: 17

Social Care Payments to Individuals and Providers – Children (Revisited)

Objective

To assess the robustness of the arrangements identified in the previous memo issued in June 2018, in ensuring that accurate and timely social care payments are made to individuals and providers.

Summary

Work is underway to move the final payment streams being made via the Children's Payment Database onto the Liquid Logic (LCS) and ContrOCC¹ systems where segregation of duties between requests, authorisation and payment can be enforced. Interim arrangements are being introduced to ensure the ongoing accuracy of payments generated via the Children's Payment Database, including increased review of:

- proposed payments within the Department for People's Finance Team
- actual payments made compared to original requests by the social care service areas.

Increased review of payments is also being introduced by the Foster Care team to confirm the ongoing accuracy of foster care fees which are actioned directly via the finance module (ContrOCC) by the Department for People's Finance Team. Again, the longer term solution, which is also part of the wider piece of work identified above, is to have the end to end process on LCS and ContrOCC, to match the arrangements in place for paying foster care allowances and expenses. As such, the process will automate the workflow for approval and reduce manual intervention.

¹ Finance module that interfaces with LCS to facilitate payments

Appendix 2B: Audit Assurances and Themes

Assurance



A regular review of system permissions is to be introduced to ensure access to LCS and ContrOCC by individual officers:

- remains appropriate to current roles
- is restricted to only one system wherever possible (the exception being read only access). Where this is not possible, appropriate monitoring of permission use is to be introduced
- does not allow for one individual to perform any process end-to-end e.g. on ContrOCC, authorise payments and undertake Manual Adjustments.

The process for setting up financial approval limits on LCS and ContrOCC is well designed and aligns to the Council's Scheme of Delegation and the approach used for the Council's key financial system Business World. A report is being designed to notify all movers / leavers actioned through MyICT requests to the Department for People's Finance Team to ensure approval limits can be updated / removed as required.

Not all items requiring financial approval are automatically routed on LCS to the appropriate budget holder, instead being routed to the line manager. This is a known glitch of the LCS system and line managers are expected to identify and re-route financial approvals beyond their corporate delegated approval limits to the budget holder. A report has been developed to identify those that have not been re-routed and resulted in line managers authorising beyond their designated approval limits. Regular review of this by the Heads of Service and the Director of Children's Services will allow for any inappropriate authorisations to be identified and addressed as necessary.

Developing a central record of care contributions agreed by Health and Education partners will:

- ensure all agreed contributions are known
- allow for uplifts in placement costs to be reflected in reclaims
- give added assurance that all agreed contributions are being reclaimed.

This page is intentionally left blank

Appendix 2C: Other Audits and Grant Claims

Objective

To confirm that grant allocations for 2018/19 received from the Department for Transport and the Ministry of Housing, Communities and Local Government have been spent in accordance with the relevant scheme's terms and conditions.

Disabled Facilities Capital Grant Determination (DFG)

Purpose of funding

To support those in non-council properties with required adaptations to their homes based on their medical needs. Types of works undertaken include installations of:

- level access showers
- ramped access to properties
- stair lifts or through-floor lifts.

Conclusion

It was confirmed that spend was compliant in that:

- it fell within the definition of "capital" for accounting purposes
- grant monies had been transferred into the local Better Care Fund pooled budget, under Section 75 of the NHS Act 2006.

In addition, work was undertaken to verify that all cases were supported by:

- an assessment of need and recommendation of adaptation works required, undertaken by an Occupational Therapist
- suitable means testing to ensure eligibility to the DFG scheme, where required
- a signed agreement from surveyors and clients that works had been completed as per the plans, and to a suitable standard.

Opinion: Unqualified

Appendix 2C: Other Audits and Grant Claims

Highways Maintenance Challenge Fund

Purpose of funding

Funding was provided to assist with highway flood reduction and resilience.

Conclusion

It was confirmed that spend was compliant in that:

- it fell within the definition of "capital" for accounting purposes
- work undertaken related to highway flood reduction and resilience in the borough.

Opinion: Unqualified

National Productivity Investment Fund

Purpose of funding

Funding was provided to support the town centre redevelopment improvement project.

Conclusion

It was confirmed that spend was compliant in that:

- it fell within the definition of "capital" for accounting purposes
- work undertaken related to town centre redevelopment.

Opinion: Unqualified

Appendix 2C: Other Audits and Grant Claims

Local Transport Capital Block Fund

Purpose of funding

To assist in delivering transport improvement schemes, which can include:

- road markings and re-surfacing
- upgrades to traffic signal junctions, zebra and puffin crossings
- bridge strengthening
- installation / replacement of sign lights and street lights
- upgrades to electronic bus information screens
- pothole repairs.

Conclusion

It was confirmed that spend was compliant in that it fell within the definition of "capital" for accounting purposes.

Some issues were identified that did not impact on the ability to confirm the grant expenditure, but required attention from the service area. Evidence that works had been completed, such as records of site visits or photos showing works completed, were not always available. Work was undertaken by engineers to re-visit works and verify that they had been completed in line with the invoices paid.

Opinion: Unqualified

Troubled Families Programme, Payments by Results Scheme Grant

Objective

To assess compliance with the terms and conditions of the Ministry of Housing, Communities and Local Government's (MHCLG) Financial Framework for making Payment by Result (PBR) claims under the Expanded Troubled Families Programme (Phase 2).

Background

The Financial Framework requires that Internal Audit verifies a 10% representative sample of PBR claims before they are made to ensure there is supporting evidence to confirm families:

- met the required criteria to be considered for entry to the expanded Troubled Families Programme
- have achieved either continuous employment or significant and sustained progress as defined by the Council's agreed Outcomes Plan.

Larger sample sizes may be required for smaller claims in order to ensure the audit is meaningful.

Appendix 2C: Other Audits and Grant Claims

Conclusion

Between July and September, 48 PBR claims were presented for audit prior to submission to the MHCLG.

The Team Manager reviews a minimum of 10% of claims to confirm appropriate evidence has been provided.

Of the 48 claims presented, the Team Manager reviewed 10. Internal Audit randomly selected six claims for review, which included two checked by the Team Manager. For all but one claim, suitable evidence was available to support:

- entry into the programme
- a claim for either significant and sustained progress, or continuous / subsequent employment.

One claim submitted under the significant and sustained progress outcome was withdrawn as whilst the mother had engaged with the Community Mental Health Team, evidence was not available to demonstrate her engagement with substance misuse agencies for the required number of sessions, or a reduction in her cannabis use as required by the Council's Outcome Plan.

This is only the second case that has been withdrawn since September 2018 which demonstrates that the Team Manager's quality assurance checks are working effectively. This has also been confirmed from the findings of the MHCLG's recent spot check process – see below.

Claims Validation 'Spot Check' Process

During August, the programme was subject to its second spot check from the MHCLG. The MHCLG conducts a validation process to ensure claims are compliant with the terms of the programme's financial framework, including checking evidence of eligibility, successful outcomes and whole family working'

The MHCLG concluded there were no invalid claims and confirmed they 'are confident the team are working within the principles of the programme's financial framework'. The MHCLG recognised that the 'services in Southend-on-Sea work hard to support families with complex and high-level needs to make sustainable changes in their lives'.

Appendix 2D: Follow up audits

Purpose of these audits

To assess whether the actions agreed in the original audit report have been implemented and are now effectively embedded into the day-to-day operation of the service.

Management Response to Quality Assurance audits

Original Objective

To assess whether senior managements revised arrangements for ensuring prompt action is taken to address the improvements required where a children's social care file is assessed as 'inadequate' or 'inadequate critical', are operating effectively to minimise the risk to Children.

Results

| Fully implemented | Substantially implemented | Partially implemented | Not implemented |
|-------------------|---------------------------|-----------------------|-----------------|
| 2 | 1 | 4 | 4 |

Summary

| Period | No. of Audits | No. of Inadequate | No. of Repeat Inadequate |
|----------------------|---------------|-------------------|--------------------------|
| June 2018 – May 2019 | 219 | 8 3.7% | 0 0% |

The stages for improving practice detailed within the 'Departmental Response to Audits' process (the process) remain well designed. If consistently applied the process aims to ensure the robustness of action taken to improve social work practice for children whose case files are assessed as inadequate.

Since the original audit, the process has been updated to reflect areas where there is some flexibility to move away from the process e.g. where the criteria for a full caseload review of a social worker's caseload has been met but deemed not to be required.

Further updates are required to:

- ensure cover arrangements are followed when the Practice Lead is out of the office and the day three meeting is going to be missed
- make clear the requirements of managers to proactively monitor cases found to be inadequate to ensure remedial actions are happening consistently and are effective.

A monitoring spreadsheet has been developed and is well designed to give adequate oversight of the key stages of the process and whether they are being met. Introducing dedicated administrative support to regularly review the spreadsheet against the Case Management System Liquid Logic (LCS) will help ensure any deviation from, or delay in the process will be highlighted quickly and can be escalated as necessary.

Appendix 2D: Follow up audits

The improvement process remains focused on the practice of the Social Workers responsible for cases. There is opportunity to extend this to other professionals and their roles in cases, such as Team Managers and Independent Reviewing Officers.

Outlining how these are addressed, managed and reported (e.g. in a similar way to how practice issues relating to Social Workers are addressed through the Whole Caseload Review process) will help to improve practice across the department where required.

Until November 2018 there was monthly reporting to the Director of Children's Services on the results of Quality Assurance audits but these are on hold while the role of the new Practice Unit is developed. These reports provided:

- overall file gradings following new audits and re-audits of previously inadequate cases
- a breakdown of grading's against various audit themes, such as 'voice of the child'.

There is limited information about the process reported within these, with the exception of November's report where more information was given on:

- manager performance in responding to monitoring and reviewing plans in line with the process (i.e. Service Manager review within 10 days) and the timeliness of response to the case found to be inadequate in that month
- work being undertaken to improve the notification process, including engagement with Managers to better understand what they need to support them effectively monitor the implementation of improvement plans.

Reintroducing consistent reporting inclusive of feedback on adherence to the improvement process will allow the Director of Children's Services to:

- get assurance the process is working effectively and consistently
- challenge where the agreed process has not been followed.

Due to the lower number of inadequate cases, this will be reported formally on a quarterly basis. The Head of Children's Services Transformation will provide updates on the progress of individual cases to the Director of Children's Services as required.

Appendix 3: Stakeholder Surveys, Compliance with Professional Standards

| Setting up and planning the audit (PSIAS 1200 / 2200) | | |
|--|---|------|
| 1 | Did we show a good level of knowledge and understanding of your service when discussing the potential scope and objective to be covered by the audit before fieldwork took place? | 100% |
| Performing the audit (PSIAS 2300) | | |
| 2 | Did we work effectively with you when doing the audit to minimise the impact on your service? | 100% |
| 3 | Were we able to talk knowledgeably with you about information provided to us and queries we had during the audit? | 93% |
| Communicating results (PSIAS 2400) and Improving governance, risk management and control processes (PSIAS 2100) | | |
| 4 | Did we keep you informed of the progress of the audit and issues arising from the work in timely manner? | 92% |
| 5 | Did we effectively explain to you where we felt action was required to improve your arrangements and why? | 100% |
| 6 | Was the report fair and reflective of the work done by audit and the issues found as discussed with you? | 93% |
| Independence and Objectivity (PSIAS 1100) | | |
| 7 | Did we provide relevant evidence to back up our findings if required? | 100% |
| 8 | At the end of the audit, did you understand the rationale for the overall opinion given? | 100% |
| Managing the Internal Audit Activity (PSIAS 2000) | | |
| 9 | Do you think internal audit adds value to the Council? | 100% |

This page is intentionally left blank

CIPFA Better Governance Forum

Audit Committee Update

Helping Audit Committees to Be Effective

Issue 29

CIPFA Statement on the Role of the Head of Internal Audit

External Audit Arrangements for English Local Government Bodies

Regular Briefing on Current Issues

August 2019

Introduction

Dear audit committee member,

This is the 29th issue of Audit Committee Update. Our main focus in this issue is the new CIPFA Statement on the Role of the Head of Internal Audit in Public Service Organisations. The Statement was published in April and helps audit committee members to understand what they should expect from the head of internal audit. It also sets out the overview and support that the audit committee should provide to that role. It is therefore a key document in understanding the role that internal audit should be playing within the organisation.

The remainder of this issue focuses on keeping you up to date with new developments. There are some important developments that will impact on the work of audit committees, particularly in relation to local audit in England. Our briefing highlights the key reports and work in progress, and we will keep you updated in future issues.

Overall, I hope that you find this issue interesting, informative and helpful in your work on the committee.

Best wishes

Diana Melville

CIPFA Better Governance Forum

Sharing this Document

Audit Committee Update is provided to subscribers of the Better Governance Forum for use within their organisations. Please feel free to circulate it widely to your organisation's audit committee members and colleagues. It can also be placed on an intranet. It should not be shared with audit committee members of organisations that do not subscribe to the Better Governance Forum or disseminated more widely without CIPFA's permission.

Audit Committee Update is covered by CIPFA's copyright and so should not be published on the internet without CIPFA's permission. This includes the public agendas of audit committees.

Receive our Briefings Directly

This briefing will be sent to contacts of organisations that subscribe to the CIPFA Better Governance Forum, with a request that it be sent to all audit committee members.

If you have an organisational email address (for example jsmith@mycouncil.gov.uk) then you will also be able to register on our website and download any of our guides and briefings directly. To register now, please visit www.cipfa.org/Register. To receive mailings from the Better Governance Forum you will need to opt-in. See My Preferences under 'My CIPFA' on the website one you have logged in.

Previous Issues of Audit Committee Update

You can download all the previous issues from the CIPFA Better Governance Forum website. Click on the links below to find what you need.

| Principal Content | Link |
|---|--------------------------|
| Issues from 2010 and 2011– the content in these issues has been replaced by more recent issues. | |
| Issues from 2012 | |
| Assurance Planning, Risk Outlook for 2012, Government Response to the Future of Local Audit Consultation | Issue 7 |
| Commissioning, Procurement and Contracting Risks | Issue 8 |
| Reviewing Assurance over Value for Money | Issue 9 |
| Issues from 2013 | |
| Public Sector Internal Audit Standards and Updates to Guidance on Annual Governance Statements | Issue 10 |
| Local Audit and Accountability Bill, the Implications for Audit Committees, Update of CIPFA's Guidance on Audit Committees | Issue 11 |
| Reviewing Internal Audit Quality, New CIPFA Publication, Audit Committees Practical Guidance for Local Authorities and Police, Regular Briefing on Current Issues | Issue 12 |
| Issues from 2014 | |
| Reviewing the Audit Plan, Update on the Local Audit and Accountability Act, Briefing on Topical Governance Issues | Issue 13 |
| Issues 14 and 15 – the content in these issues has been replaced by more recent issues. | |
| Issues from 2015 | |
| What Makes a Good Audit Committee Chair? Governance Developments in 2015 | Issue 16 |
| The Audit Committee Role in Reviewing the Financial Statements, Regular Briefing on Current Developments | Issue 17 |
| Self-assessment and Improving Effectiveness, Appointment and Procurement of External Auditors, Regular Briefing on Current Issues | Issue 18 |
| Issues from 2016 | |
| Good Governance in Local Government – 2016 Framework, Appointing Local Auditors, Regular Briefing on Current Issues | Issue 19 |
| CIPFA Survey on Audit Committees 2016, Regular Briefing on Current Issues | Issue 20 |
| The Audit Committee and Internal Audit Quality, Briefing on Topical Issues | Issue 21 |
| Issues from 2017 | |
| Developing an Effective Annual Governance Statement, Regular Briefing on Current Developments, Audit Committee Training | Issue 22 |
| 2017 edition of the Public Sector Internal Audit Standards, Risks and Opportunities from Brexit, Recent Developments and Resources | Issue 23 |

| | |
|---|--------------------------|
| Issues from 2018 | |
| The Audit Committee Role in Risk Management, Regular Briefing on Current Developments | Issue 24 |
| Developing an Effective Annual Governance Statement | Issue 25 |
| CIPFA Position Statement on Audit Committees in Local Authorities and Police 2018 | Issue 26 |
| Issues from 2019 | |
| Focus on Local Audit National Audit Office Report: Local Authority Governance | Issue 27 |
| The Audit Committee Role in Counter Fraud | Issue 28 |

Workshops and Training for Audit Committee Members in 2019/20 from CIPFA

Introduction to the knowledge and skills of the audit committee

This training course will provide more in-depth knowledge of the core areas of an audit committee's functions, including risk management, assurance planning and improving the effectiveness of the committee.

- [18 September, London](#)
- [19 September, Leeds](#)
- [17 October, Birmingham](#)

Development day for police audit committees

These events are suitable for members of the joint audit committees supporting police and crime commissioners (PCCs) and chief constables. These events are run in conjunction with CIPFA's Police Network.

- 21 November, York
- 28 November, London

Development day for local government audit committees

This workshop is suitable for audit committee members or those working with the audit committee in local government. It will cover an update on new developments and guidance relevant to the audit committee role. In addition, it will feature key topics for the audit committee agenda.

- 13 November, London
- 4 December, Birmingham

Other dates in late 2019 or early 2020 will be announced later in the year.

The above events can all be accessed using prepaid places for the CIPFA Better Governance Forum. CIPFA events information and dates will be available on the [website](#) in due course.

CIPFA events information and dates are available on the website: www.cipfa.org/Events.

In-house training and facilitation

In-house audit committee training and guidance tailored to your needs is available. Options include:

- key roles and responsibilities of the committee
- effective chairing and support for the committee
- working with internal and external auditors
- public sector internal audit standards
- corporate governance
- strategic risk management
- value for money
- fraud risks and counter fraud arrangements
- reviewing the financial statements
- assurance arrangements
- improving impact and effectiveness.

For further details contact diana.melville@cipfa.org or visit the [CIPFA website](#) for further details on the support we have available for audit committees.

CIPFA Statement on the Role of the Head of Internal Audit – what does the audit committee need to know?

The [CIPFA Statement on the Role of the Head of Internal Audit in Public Service Organisations](#) was published in April 2019. It is aimed at audit committees and leadership teams, helping them to understand the role of the head of internal audit and the organisational arrangements that should be in place to provide effective support to the role.

The audit committee plays a key role in relation to internal audit, providing oversight of the arrangements for the service and holding it to account for its delivery of the audit plan. It also plays a vital role in providing high-level support and helping to ensure that its reports and recommendations are considered and addressed by managers. A talented head of internal audit can do a very good job in organising his or her team and ensuring professional internal audit standards are met, but unless there is the right level of engagement with the audit committee and leadership team the impact and effectiveness of internal audit is likely to be undermined. Therefore, it is important that the audit committee understands its role and plays it effectively.

Structure of the Statement

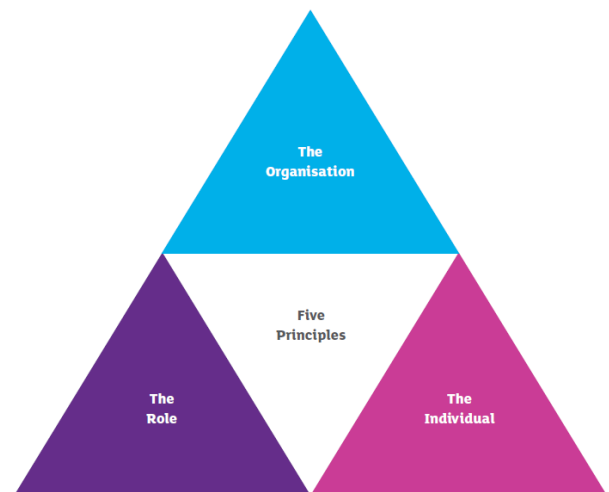
The Statement has five principles that should be applicable to any public sector organisation. For each principle the organisational arrangements are identified along with the characteristics of the role and of the individual. The principles are aligned to the professional standards for internal audit: the Public Sector Internal Audit Standards (PSIAS).

The head of internal audit in a public service organisation plays a critical role in delivering the organisation's strategic objectives by:

1. objectively assessing the adequacy and effectiveness of governance and management of risks, giving an evidence-based opinion on all aspects of governance, risk management and internal control
2. championing best practice in governance and commenting on responses to emerging risks and proposed developments.

To perform this role the head of internal audit must:

3. be a senior manager with regular and open engagement across the organisation, particularly with the leadership team and the audit committee
4. lead and direct an internal audit service that is resourced appropriately, sufficiently and effectively
5. be professionally qualified and suitably experienced.



Key steps for the audit committee member

CIPFA recommends that audit committee members should read the Statement, as it helps them to understand more about the role and responsibilities of the head of internal audit. Of particular interest to the audit committee member will be the following areas:

- Clear designation of who holds the position of head of internal audit (Principle 3). Sometimes in contracted or shared services this individual may not be a direct employee of the organisation, so it is important to be clear where responsibility lies.
- How the head of internal audit reports to the audit committee (Principle 1).
- Which member of the leadership team has responsibility for internal audit (Principle 1).
- Whether the internal audit charter and plan have been approved by the audit committee (Principle 1).
- Whether the head of internal audit has direct access to the audit committee and members of the leadership team (Principle 3).
- The audit committee terms of reference should include oversight of internal audit and monitoring of adherence to professional standards (Principle 3).
- Whether the head of internal audit has the status, resources, expertise and systems needed to perform the role effectively (Principle 4).
- Ensuring that the audit committee supports the head of internal audit and participates in the service's quality assurance and improvement programme (Principle 4).
- Support for the head of internal audit to maintain professional knowledge and extend skills and knowledge (Principle 5).

If the organisation is recruiting a new head of internal audit then the chair of the audit committee may be briefed about the selection process or may participate in the selection. The Statement also includes the personal skills and professional standards that the head of internal audit is expected to meet, and these may be helpful in supporting the selection process.

Additional guidance

To accompany the Statement CIPFA has also published a set of case studies demonstrating how heads of internal audit are putting the principles of the Statement into practice. The examples include supporting the development of the audit committee, reviews of governance arrangements and coaching internal audit team members. Leading Internal Audit can be downloaded from the [CIPFA website](https://www.cipfa.org/leading-internal-audit) and we hope that it will provide further support in understanding the role and potential of the head of internal audit.

Putting the Statement into practice

The committee can use the Statement when it reviews internal audit agenda items at its meetings, for example, an update of the internal audit charter or consideration of the annual opinion and report. The Statement can also inform the committee's review of its own terms of reference, preparation of an annual report or self-evaluation.

Diana Melville

Governance Advisor

CIPFA Better Governance Forum

External Audit Arrangements for English Local Government Bodies

Whilst external arrangements for local government in Wales, Scotland and Northern Ireland have remained stable over the last ten years, arrangements for English bodies: councils, police and fire and rescue organisations, have gone through significant change. And more is set to come.

Minister of State Eric Pickles announced the intention to close the Audit Commission, which had overseen external audit arrangements, in 2010. Whilst some immediate changes such as the cessation of the Comprehensive Area Assessment and the Use of Resources assessments happened straight away, other changes took time to implement. External audits performed by the District Audit team of the Audit Commission were outsourced. The Local Audit and Accountability Act was passed in 2014. Public Sector Audit Appointments was established firstly to oversee the management of the contracts let by the Audit Commission. It was then authorised to conduct a procurement of audit services that local government bodies could choose to opt into. Over 98% of local bodies did choose to do so. Those contracts were let in 2017 to start for the 2018/19 financial year. So only now are the first audits being conducted under the devolved system envisaged by the Act.

The regulation of local auditors also changed under the Act. The Code of Audit Practice, which provides the more detailed framework of the scope of the audit, is now led by the National Audit Office (NAO). The Financial Reporting Council (FRC) was given a new role in relation to audit quality.

Current issues and challenges

Timely completion of the audit

Some organisations are experiencing delays with the completion of their audit because of capacity issues within the audit firms. Recent press reports include an article in [Local Government Chronicle](#) about the impact on 19 councils; but other bodies are likely to be affected.

Satisfaction with the audit process

The recent report from the National Audit Office, [Local Authority Governance](#) included concerns from some of the organisations being audited that the audit provides less in-depth assurance, particularly around governance and the use of resources, than they would like.

Another concern expressed is that prices may have been reduced too much and the quality of audit has suffered as a result. In the NAO's survey a quarter of respondents from single tier and county councils felt their fees were too low relative to the risk that their authority faces.

Similar comments were made in the consultation on the NAO's Code of Audit Practice.

Concerns that audit recommendations do not have the expected impact

In their report on [Local Auditor Reporting](#), the NAO expressed concerns that adverse auditor reports or recommendations were not responded to effectively by the organisations affected and that the impact of a qualified conclusion on value for money appeared to be limited.

Impact of audit issues beyond the public sector

Auditors in the private sector have also faced criticism. For example the auditors of Carillion and Patisserie Valerie are currently under review to ensure that those audits met the standards expected. Whilst these issues relate to private sector audits, inevitably any concerns about the quality and reliability of audit do have an impact more widely.

Another issue is the competitiveness of the audit market and maintaining auditor independence. The independent appointment of auditors in local government has helped the sector avoid the accusation that auditors are too close to the organisations they audit. By contrast, some major companies have retained the same audit firm for more than a decade.

Ensuring effective regulatory reporting

A new role for the Financial Reporting Council (FRC) is to review audit quality in a similar way to the audit quality reviews that they undertake on the firms' corporate client audits. Corporate audit committees receive a report from the FRC on the results of their quality review of the company's audit if one is undertaken. A similar approach would be a new responsibility for a local government audit committee.

Recent reviews and recommendations on external audit

Review of local authority financial reporting and external audit, the Redmond review

This review, chaired by Sir Tony Redmond, was announced by James Brokenshire in July. The review has a broad remit to consider the impact of the changes made by the Local Audit and Accountability Act, plus wider issues around public reporting and the transparency of financial reporting. The review will consider arrangements within all aspects of local government: authorities, police, fire authorities and also smaller authorities. It will not consider the audit of health trusts even though the Act also applied to those bodies.

The [terms of reference](#) of the review have been published by the Ministry of Housing, Communities and Local Government. Whilst the review as a whole will be of interest to audit committees, it is worth noting that the review will consider how effectively local government bodies engage with and respond to audit recommendations. This will of course focus on the role played by the audit committee.

The review will involve consultation with a range of stakeholders, including authorities.

Consultation on the Code of Audit Practice

Earlier this year the National Audit Office published an issues paper to seek views on how it should revise the Code of Audit Practice. The NAO has now published a [summary paper](#) discussing the responses it received and setting out its next steps. There will be further consultation late in the year on the draft of the Code. The latest paper indicates that there will be a greater emphasis on the auditor's assessment of value for money arrangements. This is potentially a helpful change that will provide audit committees with greater insight and assurance.

Market study on statutory audit services: initial consultation

The government recently published [proposals](#) on how it intends to implement the recommendations made by the Competition and Markets Authority on the audit market. The proposals include promoting competition in the audit market through joint audits and ensuring operational splits between audit and non-audit work. There are also recommendations for greater scrutiny from the regulator over the appointment of auditors by the audit committee.

The firms that conduct local audit will be impacted by these proposals in their wider audit work and the proposals could have direct implications for local audit. Further clarity is required on this.

The quality and effectiveness of audit: independent review

The Department of Business Energy and Industrial Strategy (BEIS) has initiated a review, known as the [Brydon review](#), to look at audit scope and reporting across the corporate

sector. It is included here as any recommendations impacting on audit will have some influence on those arrangements in other sectors, including the public sector.

Independent review of the Financial Reporting Council 2018 (Kingman report)

This [report](#) was commissioned by (BEIS) and focused on the role of the FRC. It included arrangements for the regulation of local audit. The report recommended that the FRC should be replaced with a new body, the Audit, Reporting and Governance Authority. It also made recommendations for a fundamental rethink of local audit arrangements and to bring together all regulatory responsibilities for local audit under a single body.

In his response to the report, the secretary of state said that the recommendations relating to the regulation of local audit would be addressed separately. The Redmond review will address these aspects within its scope.

So what does this mean for local government?

In summary, the future shape of local audit arrangements is fluid. It seems likely that the proposals will seek to strengthen and improve the impact of local audit. For local bodies this could mean more rigorous scrutiny on key risks to value for money, for example financial sustainability or the adequacy of governance arrangements. It is also likely that local bodies will be expected to ensure that their arrangements to engage with the auditors and to receive and respond to auditor recommendations, including the audit committee, are sufficiently robust.

It is too early to speculate whether there will be changes to the appointment mechanism of local auditors. Changes to the current arrangements would require primary legislation and so could not happen quickly.

Steps for audit committees to take now

1. Continue to monitor the current reviews and take opportunities to respond to consultations.
2. Engage effectively with your current local auditor. Where there are issues with delivery (such as a delay in completion of the audit) ensure that they are raised with the engagement partner responsible and with PSAA.
3. Respond effectively to recommendations raised by the local auditor. Monitor the implementation of any action plan to ensure the necessary changes are made.
4. Ensure you have a robust framework for internal assurance. The local auditor's opinion and report are just one source of assurance, albeit a very important one. Audit committees should be clear about how they get assurance and how robust these arrangements are. Pay attention in particular to the Annual Governance Statement, the head of internal audit's annual opinion on governance, risk management and internal control and the quality of your risk management arrangements.
5. If you haven't already done so, complete an evaluation of your audit committee's effectiveness. Are you fulfilling the requirements of your terms of reference and does your work have impact? Do you need any further support in performing your role? [Issue 18 of Audit Committee Update](#) and CIPFA's publication, [Audit Committees Practical Guidance for Local Authorities and Police](#) contain guidance on undertaking a self-assessment of the audit committee. Alternatively, ask your head of internal audit for advice.

Diana Melville

Governance Advisor, CIPFA Better Governance Forum

Recent Developments You May Need to Know About

Regulations

Overview and scrutiny: statutory guidance for councils and combined authorities

The new [guidance](#) includes policies and practices authorities should adopt or should consider adopting when deciding how to carry out their overview and scrutiny functions. The guidance does not apply to audit committees but will be of interest to Councillors in their wider scrutiny roles or for understanding the contribution scrutiny makes to the effectiveness of governance.

Consultations

Consultation on the Code of Audit Practice

The NAO has published its [response](#) to the consultation earlier this year on the development of the new Code. Further consultation will take place in the autumn as the new Code must be approved by Parliament for implementation from April 2020.

CIPFA consultation on simplifying the accounts

CIPFA is conducting a survey on local authority accounts and wants users, such as audit committee members, to complete a short online survey. The results of the survey will be used to inform CIPFA's work to streamline the accounts and improve their accessibility for users. The online survey can be accessed [here](#).

Reports, recommendations and guidance

Public Accounts Committee report: local government governance and accountability

The Public Accounts Committee has concluded that the government has not done enough to ensure that, at a time when local authority budgets are under extreme pressure, governance is improved. The committee found that in some authorities governance is under strain: audit committees that do not provide sufficient assurance, ineffective internal audit, weak arrangements for the management of risk in local authorities' commercial investments, and inadequate oversight and scrutiny.

The committee has recommended that the department should assess the governance evidence base available to it and write to them by November 2019, setting out how it will address gaps it has identified. [Public Accounts Committee](#)

Safeguarding public money: are you getting it right?

Guidance from the Accounts Commission in Scotland emphasises the importance of councillor scrutiny of financial safeguards. The report explains the importance of internal controls for managing risk and highlights how mistakes and fraud can happen if controls are weak. The report also covers the roles of internal audit and the audit committee and includes a checklist of key questions. It is a useful resource for all public bodies. [Safeguarding public money](#)

Fraud and irregularity update 2018/19

A summary of the cases of fraud and other irregularities at public bodies in Scotland. Common internal control weaknesses had provided the opportunity for the frauds to take place and public bodies are recommended to review their arrangements. [Audit Scotland](#)

Counter-fraud arrangements in the Welsh public sector

An overview for the National Assembly's Public Accounts Committee of the counter-fraud landscape across the Welsh public sector. [Wales Audit Office](#)

CIPFA Fraud and Corruption Tracker

CIPFA has completed its annual survey of levels of fraud and corruption detected across the public sector in the 2018/19 financial year. The results of this survey will be published in the autumn and will provide a valuable insight into current levels of detected fraud and corruption. [CIPFA Fraud and Corruption Tracker](#)

Policing and fire governance: guidance for police and crime panels

The Local Government Association has published guidance on governance for police and crime panels to provide information about the statutory roles of panels and to highlight good practice. The guidance does not include any reference to the work of police audit committees. [Police and crime panels](#)

Local Enterprise Partnerships: an update on progress

The NAO has published a report reviewing progress in the improvement of governance and assurance. They conclude that the assurance framework is stronger, but it is not yet proven whether it will be effective in detecting and responding to governance failures. [National Audit Office](#)

Guidance for audit committees on cloud services

The NAO has published a guide to brief public sector audit committees about the use of cloud services. It suggests questions to ask at the planning, implementation and management stages. [National Audit Office](#)

Financial Foresight

Grant Thornton and CIPFA have produced a report, [Financial Foresight](#), providing insights into financial sustainability at English local authorities. Understanding the issues will help councils in their longer term financial planning.

Local Audit Quality Forum

The Forum is run by Public Sector Audit Appointments to support council and police audit committees in their role. [Presentations](#) from the June 2019 Forum held in London are now available.

Local government in Scotland: Challenges and performance 2019

A [report](#) from Audit Scotland reviewing the performance of Scotland's councils. It reports that most are managing to improve and maintain services but there are challenges ahead.

Local Government Auditor's Report 2019

This [report](#) from the Northern Ireland Audit Office comments on a range of topics arising from audit work in local government bodies during the 2018/19 financial year. It highlights areas of strength and areas for improvement within local councils.

Developments to Look Out For

New CIPFA Financial Management Code

In the autumn CIPFA will be publishing the Financial Management Code (FM Code). The FM Code is designed to support good practice in financial management and to assist local authorities in demonstrating their financial sustainability. For the first time The FM Code sets out the standards of financial management for local government.

The FM Code includes the CIPFA Statement of Principles of Good Financial Management. These six principles have been developed by CIPFA in collaboration with senior leaders and practitioners who work within or have a stake in good local authority financial management. These principles are the benchmarks against which all financial management should be judged. CIPFA's view is that all financial management practices should comply with these principles.

The FM Code will apply from April 2020, but authorities are encouraged to ensure that their preparation of the 2020/21 budget and longer term strategies and plans aligns to the FM Code.

Published by:

CIPFA \ THE CHARTERED INSTITUTE OF PUBLIC FINANCE AND ACCOUNTANCY

77 Mansell Street, London E1 8AN

020 7543 5600 \ www.cipfa.org

© 2019 CIPFA

No responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication can be accepted by the authors or publisher.

While every care has been taken in the preparation of this publication, it may contain errors for which the publisher and authors cannot be held responsible.

Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may be reproduced, stored or transmitted, in any form or by any means, only with the prior permission in writing of the publishers, or in the case of reprographic reproduction in accordance with the terms of licences issued by the Copyright Licensing Agency Ltd. Enquiries concerning reproduction outside those terms should be sent to the publishers at the above mentioned address.

10

Document is Restricted

This page is intentionally left blank