Southend-on-Sea Borough Council

Agenda Item No.

Report of the Executive Director (Transformation)

to

Audit Committee

on

21 October 2020

Report prepared by: Val Smith, Knowledge and Data Privacy Manager/Data Protection Officer

Risk Assurance – Data Protection in a Time of Pandemic

A Part 1 Public Agenda Item

1. Purpose of Report

1.1 To advise the Audit Committee on the measures being taken by Southend-on-Sea Borough Council concerning data protection in the context of the coronavirus pandemic.

2. Recommendations

2.1 **The Audit Committee notes the measures being taken to protect personal data during the coronavirus pandemic.**

3. Background

3.1 On 15 September 2020 the Information Governance Update and Senior Information Risk Owner (SIRO) Annual Report 2019/20 was presented to Cabinet.

3.2 The report included a future programme of work, highlighting that the coronavirus pandemic had necessitated a revision of priorities regarding data protection and cyber security.

3.3 This report provides an explanation of how the Council is protecting the personal data of citizens when conducting its business.

3.4 Located within the Corporate Strategy Group (Transformation), the Information Governance team, led by the Council’s Data Protection Officer, provide direction, advice, guidance and governance to the organisation.

3.5 Located within ICT as part of Transformation, the IT Security function provides policy, guidance and technical and organisational measures to protect the Council’s networks, systems, supply chain, users and data in line with industry and government standards.

3.6 Information Governance and ICT Security work together to ensure data protection and cyber security related actions are complementary and, wherever relevant, are jointly delivered and / or communicated.

4. Risk Assessment and Assurance – Coronavirus Activities

4.1 As a result of the coronavirus pandemic emergency many new initiatives have had to be implemented at speed.

4.2 The Council's Data Protection by Design and Default policy explains that new or amended procedures which involve the use of personal data must be designed from the outset to ensure that people's rights concerning their personal data are respected. There are several mechanisms which help ensure the necessary thought processes take place before personal data is processed.

4.3 An Initial Data Protection Risk Assessment is conducted by the Information Governance team to determine the potential level of risk to personal data. For higher risk initiatives, a detailed Data Protection Risk Assessment is required. For lower risk proposals, a Data Protection Compliance Check is conducted.

4.4 Whichever method is appropriate, the Information Governance team will assess the proposal against all data protection legislative requirements, calling on ICT specialists for the assessment of any aspects relating to their field.

4.5 Only once the data protection risks and requirements have been assessed and sufficiently mitigated will processing of personal data commence. In addition to consideration by Information Governance and ICT, higher risk processing will be authorised by the Senior Information Risk Owner (SIRO) and / or the Caldicott Guardian.

4.6 Where a proposed activity requires the sharing of personal data with others (such as with local partners, the NHS, central government, fellow Councils) it is important that all those concerned understand the purpose for which the personal data is being shared and the limitations on its use. This ensures that data is only used in ways that the people concerned would think are reasonable and fair.

4.7 Some data with which we have been provided to help us reach individuals because of the pandemic, particularly by the NHS regarding 'shielded' individuals, is highly sensitive and only given to us for very specific purposes. This has had to be tightly 'locked down' even within the Council to ensure data security. For all data sharing, only the minimum amount of data needed to carry out the purpose must be shared.

4.8 Whenever personal data is to be shared on a regular basis, the Information Governance team support the production of a formal Information Sharing Agreement which details the purpose and limit of the sharing, its legislative basis and the roles and responsibilities of those concerned. Where another agency is leading on the Information Sharing Agreement, the Information Governance Team will provide assurance whether the agreement meets data protection requirements and ensure the Council's part of the arrangement is robust.

4.9 The Government published new legislation to allow greater data sharing for coronavirus related purposes (Control of Patient Information notice - COPI 3(4) notice, Health Service Control of Patient Information Regulations 2002) and this has been analysed and applied to the initiatives with which the Council is concerned.

4.10 Information Sharing Agreements are authorised by the project lead, the appropriate Manager, or the Information Governance Advisor as appropriate. Where the sharing is of sensitive social care data, the Caldicott Guardian is the authorising person.

4.11 A privacy notice explains to individuals how their personal data will be used. This is important, not only because it is a legal requirement, but for people to trust us with their information. In addition to the overarching privacy notice for the Council, privacy notices have been produced for the new and revised uses of personal data in support of the Council's coronavirus response.

4.12 The Information Governance service also supports officers entering into contracts on behalf of the Council to ensure that appropriate clauses to safeguard personal data are included, or that clauses proposed by others are sufficient and appropriate.

4.12 These processes have been approved by the Good Governance Group and have not changed because of the coronavirus pandemic. The same level of vigilance and assurance is being applied. To provide the speed of response with which some processes have had to be introduced, it has however been necessary to prioritise this work over other duties, as explained below.

4.13 Appropriate records of the above have been kept by the Information Governance team and are available for the Information Commissioner should compliance with the Data Protection Act 2018 and GDPR need to be demonstrated.

4.14 Examples of work undertaken by the Information Governance service relating to coronavirus are included at Appendix 1.

5. Risk Assessment and Assurance – Other Activities

5.1 As explained above, the data protection impact of coronavirus related activities has been comprehensively risk assessed and assured. At the same time, the usual business of the Council has continued and required input from the Information Governance service.

5.2 As a consequence it has been necessary to prioritise the work of the service. Data protection risk assessments, Information Sharing Agreements and Privacy notices (as described above) have continued as normal with no change to the service.

5.3 The immediate assessment and mitigation of data security incidents has continued in line with regulatory requirements. No incidents have occurred requiring notification to the Information Commissioner.

5.3 Subject Access Requests have continued to be registered and acknowledged as normal, but in many cases have taken longer than usual to receive a response. In part this has been because some applicants require paper copies of their records and the Information Governance service initially, due to the pandemic, had no access to the civic offices so could not complete this type of request. The service now has occasional access, arranged when cases are ready for despatch.

5.4 The data to be sent following a subject access request is provided either by the service area, or in the case of Children's services, by specialist officers. As a result of the pandemic, many services have faced extra demands and / or have lost staff through illness or redeployment. Their core work has had to take priority over the fulfilment of subject access requests and there has been a knock-on effect on the timescale within which subject access requests can receive their response. Requesters have been kept informed but are understandably frustrated.

5.5 Similarly, Freedom of Information Requests continue to be registered and acknowledged but the response time has suffered. While the Information Commissioner has stated their intent to be a pragmatic regulator, they have recently said that they expect data controllers to be preparing recovery plans for Freedom of Information and Subject Access work which has fallen behind. Plans will be prepared for SBC, with progress monitored by the Good Governance Group. Should there be a worsening of the pandemic, it is presently unknown whether the regulator will change their position.

6. Remote Working Enablement and Cyber Security

6.1 Enabling remote working became an immediate priority when the effects of the pandemic began to be felt. The following measures have been taken by the ICT service to enable mass remote working while at the same time protecting the security of data, particularly personal data.

6.2 A threat assessment and internal security review were carried out regarding the remote working facilities in place or introduced as a result of Covid 19, along with the assessment of operational risks applicable to the ICT function.

6.3 There was an adjustment of technical controls protecting remote access to Council technology, be that in our data centres or to cloud services e.g. Office 365. Most notably multifactor authentication (MFA) was introduced to protect against risk of unauthorised access.

6.4 Investment was made in people engaged in key cyber security roles within the Council, most notably the specialist training and upskilling of ICT personnel engaged in cyber incident response and the appointment of an experienced head of function.

6.5 Subject matter expertise was provided to support the rapid procurement and deployment of technology solutions in support of the Covid-19 response, ensuring adherence to security standards.

6.6 Cyber strategy and roadmaps were developed that outline the Councils approach to enhancing capability and maturity within the organisation with a goal to increase cyber resilience over time.

6.7 ICT supported the Governance, Risk and Audit functions in relation to cyber security through the Good Governance Group and ongoing Audit program, including the support and facilitation of a Remote Working audit.

6.8 Communications with the wider organisation were enhanced including timely cyber security related reminders, warnings and sources of further learning and information to maintain a vigilant and informed workforce. There has been sharing and collaboration of good practice and intelligence across Councils and other public sector organisations across the Essex region through the Essex Online Partnership.

7. Reasons for Recommendation

7.1 All aspects of information governance and cyber security work have continued during the pandemic. Risks are being appropriately assessed, mitigated and evidenced both for pandemic and non-pandemic related matters. Easements have been required regarding the timescale within which lesser priority work can be completed, but only in areas which do not relate to the safeguarding of personal data. Recovery plans will be prepared to recover performance in these areas as soon as practicable, given the development of the pandemic.

8. Corporate Implications

8.1 Contribution to the Southend 2050 Road Map

Information governance and cyber security work provides assurance and identifies opportunities for improvements that contribute to the delivery of all Southend 2050 outcomes.

8.2 Financial Implications

Information governance and cyber security assurance is being delivered within approved budgets. Failure by the Council to process personal data in line with legislation may lead to financial penalties from the Information Commissioner.

8.3 Legal Implications

The General Data Protection Regulation (GDPR) and Data Protection Act 2018 require data controllers to be able to evidence to the Information Commissioner their compliance with legislative requirements. This report contributes to that evidence.

8.4 People Implications

People issues identified through information governance and cyber security investigations are handled through usual channels.

8.5 Property implications

Property issues that are relevant to a data protection or cyber security matter are dealt with through the data protection by design and default process.

8.6 Consultation

Information governance and cyber security work is conducted in collaboration with service areas and overseen by the Good Governance Group. An annual report to Cabinet is made by the Senior Information Risk Owner.

8.7 Equalities and Diversity Implications

Personal data relating to protected characteristics is afforded additional protection under the GDPR and DPA 2018 and specific attention is given to the proposed use of such data before it is approved.

8.8 Risk Assessment

Failure to operate a robust assurance process (which incorporates the information governance and cyber security functions) increases the risk that there are inadequacies in the internal control framework that may impact on the Council's ability to deliver its corporate aims and priorities.

8.9 Value for Money

There are strong links between the information governance, ICT, procurement and finance services to ensure that proposed spending is directed through the correct processes. Proper consideration from the outset of data protection risk reduces the likelihood of financial penalties and reputational damage.

8.10 Community Safety Implications

These issues are only considered if relevant to a specific data protection compliance matter.

8.11 Environmental Impact

Projects with an environmental impact may also require assessment of their use of personal data.

7. Background Papers

None

8. Appendices

Appendix 1 – Examples of Coronavirus related initiatives for which data protection advice and support have been provided

Appendix 1

Examples of Coronavirus related initiatives for which data protection advice and support have been provided

Subject	Information Governance have supported the data protection elements of:
Public Health England COVID-19: Contact Tracing "Lost to Follow-Up" Pilot	PHE sharing Covid 19 positive test results for individuals so that support can be provided and test and trace carried out.
Southend BC & Essex CC Track & Trace Service - complex cases	ECC and SBC sharing data so ECC can perform the complex test and trace service on behalf of SBC.
Information sharing with GPs	SBC sharing data with GPs about high risk individuals identified from the SBC Covid response telephone line.
NHS Digital agreement	NHS Digital sharing certain information with the Council's 0-19 service to enable their work with vulnerable children to be better prioritised in a time of increased risk to vulnerable children.
Test and Trace data capture	Contact details being collected and correctly retained from visitors to all Council buildings (such as libraries, museums, community venues etc.) initially by hard copy, then by NHS App QR code capture.
Southend Coronavirus Action	The partnership between SBC, SAVS, Everyone Health and South Essex Community Hub supporting vulnerable people during the Covid 19 initial response.
Good Neighbours Scheme	Continuing to provide support to vulnerable individuals as the Coronavirus helpline was scaled back.
Cardiff University study on the impact of Homelessness and Covid-19	SBC participating in the study the University of Cardiff are doing to see if the housing needs or placement of homeless people has an impact on the spread of Covid-19.
Test and Trace local data repository	Ensuring data received from NHS Digital and central government is securely held and 'locked

	down’ to specific officers.
Rough Sleeper Initiative	Agreement between the Council and EPUT in order that help and support can be provided to the rough sleepers in relation to their mental health and wellbeing and securing of sustainable accommodation. (to reduce the risks from coronavirus).
Esri - Corona Virus Action – interactive map	On the Livewell Website, publishing a map of bodies providing support as part of the Covid-19 pandemic response.
AccuRx video consultation	Video consultation software to allow 0-19 service to conduct “virtual visits” with at risk children and families and for Health Visitor and School nurse appointments.
Local Outbreak Control Plan	The Council’s role in the event of a local outbreak of coronavirus.
Microsoft Office 365	The provision of Microsoft Office 365 functionality to the organisation, in particular remote working technology such as Teams
Remote Working Guidance	Guidance to the organisation on safe practices when working from home (supplements the 2018 Mobile Working (Home & Remote Working) procedure (jointly with Worklife and ICT)
Zoom video conferencing	Guidance on the safe use of Zoom video conferencing (largely superseded by the use of Teams)
Sharing of data from the electoral register (internally)	To be used by Operation, Performance and Intelligence team to enable coronavirus support to be provided.