Appendix 2b: Audits Revisited

Purpose of these Audits

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

Information Governance, General Data Protection Regulations

Original Objective

To assess whether the Council has an appropriate programme of work to ensure compliance with General Data Protection Regulations (GDPR) and the Data Protection Act 2018

Summary

Progress has been made in implementing the recommendations raised as part of the previous audit report dated February 2019.

Those recommendations which have been implemented to enhance the Council's compliance with the requirements of GDPR are in respect of the following areas:

- A number of GDPR-related policies have been updated in January 2020 and were subsequently approved by the Good Governance Group with future review periods outlined. The Policies are publicised on the intranet and made available to all staff.
- GDPR training, covering Data Protection and Cyber Security, for all staff has been rolled out with completion rates being reported to and monitored by the Good Governance Group.
- At the time of the audit work significant improvement in the completion of Subject Access Requests (SARs) within statutory response deadlines was noted, especially in relation to Children's services with the Good Governance Group receiving regular updates on compliance which, in turn, enables escalation processes with appropriate senior management as necessary. More recently, since the onset of the Covid 19 circumstances, it is reported that increased delays in SARs response times are being noted. The performance reporting arrangements to the GGG should ensure appropriate action is taken to address this
- The proactive use of the post-GDPR compliant Whole Essex Information Sharing Forum (WEISF) template to record new and renewed Information Sharing Agreements.
- The Information Asset Register (IAR) is now on the council's performance management system (Pentana) and can be downloaded into an Excel Spreadsheet extract as and when required.

Appendix 2b: Audits Revisited

For the remaining recommendations, management has made progress in addressing the majority of these original recommendations, but further work is required to help the Council ensure and demonstrate compliance with GDPR requirements. These include:

- Updating the current Business-As-Usual (BAU) action plan, to ensure this is an accurate record of all the work necessary to move GDPR to a BAU position and all actions are owned by officers with target dates for completion. Furthermore, the BAU plan will be updated to reflect other actions required in response to the other outstanding recommendations, including the update of the Information Asset Register.
- Arrangements to alert and prompt the review of Information Sharing Agreements for removal from Pentana, if redundant.
- Arrangements for ensuring the Information Asset Register (IAR) is an accurate and complete record of the information assets the Council holds.
- Implementing an incremental plan for the holistic review of the IAR, its components and contents. Approval of the plan by the GGG with subsequent progress reporting of completion against set timescales would improve the rigour around these arrangements. This plan was identified as a solution to support the closure of a number of the original recommendations that help inform the information presented in the IAR, specifically:

    - Prioritising areas for review such as Information Mapping within the Record of Processing Activities (ROPA) to support the process performed by management to inform the on-going completeness and accuracy of Information Mapping.

    - To identify, understand and risk assess the critical and non-critical IT systems, how the data is used, including its retention / deletion and the security of the system itself. This will inform suitable solutions for ensuring GDPR compliance of all applicable systems.

- Identifying contract managers still requiring training from a GDPR perspective and updating the GGG with progress on this. In addition, producing generic guidance on managing contracts with a GDPR element would be an incremental step in raising awareness of the necessary requirements.
- Revisiting past arrangements for identifying all contracts involving personal data at the time GDPR was introduced, and for those still live taking appropriate action to ensure the Council has met its obligations and formally confirmed its requirements for ensuring the safety of personal data held by contractors on the Council's behalf. In particular, this should cover the approach adopted for contracts below £25K and those requiring formal change control procedures as part of contractual arrangements that need to be followed. Presenting the findings to the GGG will allow appropriate challenge and risk implications to be considered.

- Agreeing a plan to implement and adopt Office 365 which has been identified as the GDPR-compliant approach to managing email to improve the way data is shared and stored. This project plan should consider all aspects applicable to rolling out a new way of working with the Good Governance Group receiving periodic updates, approving proposals around retention schedules and other decisions that impact the Council's ability to meet key requirements of GDPR.

Results

Fully implemented	Substantially implemented	Partially implemented	Not implemented
9	3	6	2