Audit Governance and Standards	**15 November 2021**

Data Protection Update

Final Decision-Maker	Audit, Governance and Standards Committee
Lead Head of Service	Angela Woodhouse Head of Policy Communications and Governance
Lead Officer and Report Author	Anna Collier Corporate Insight Communities and Governance Manager
Classification	Public
Wards affected	All

Executive Summary

Data Protection Act 2018 became law in May 2018. A key part of the Data Protection Act/UK GDPR is the accountability principle which requires organisations to have appropriate measures and records in place to be able to demonstrate compliance. An action plan has been in place since 2017 to ensure the Council was prepared for the changes and to ensure it maintains compliance. This annual update supports the Council meeting the accountability principle and ensuring a continual awareness of the national data protection landscape.

Purpose of Report

Discussion

This report makes the following recommendations to this Committee:

1. That the national context and progress to date be noted.
2. That the actions taken to date and next steps be noted.
3. That the Committee discuss the inclusion of performance data in future reports including FOI/EIR data.

Timetable	
Meeting	***Date***
Corporate Leadership Team	2 November 2021
Audit, Governance and Standards Committee	15 November 2021

Data Protection Update

1. CROSS-CUTTING ISSUES AND IMPLICATIONS

Issue	Implications	Sign-off
Impact on Corporate Priorities	Accountability supports organisations to minimise the risk to personal data held, by putting in place appropriate and effective policies, procedures and measures. By reducing risk and ensuring we have appropriate arrangements in place the Council will be able to meet our corporate objectives.	Corporate Insight, Communities and Governance Manager
Cross Cutting Objectives	The report recommendation supports the achievements of all cross-cutting objectives. It does this by ensuring that the Council collects, processes, stores and deletes residents' personal information responsibly and in accordance with the GDPR/DPA 18 whilst delivering its objectives.	Corporate Insight, Communities and Governance Manager
Risk Management	This action plan identifies actions to mitigate and manage risk in relation to the personal data held and processed by the Council.	Corporate Insight, Communities and Governance Manager
Financial	The proposals set out in the recommendation are all within already approved budgetary headings and so need no new funding for implementation.	Section 151 Officer & Finance Team
Staffing	We will deliver the recommendations with our current staffing.	Corporate Insight, Communities and Governance Manager
Legal	Accepting the recommendations will fulfil the Council's duties under the General Data Protection Regulations and the Data Protection Act 2018.	Legal Team
Privacy and Data Protection	Accepting the recommendations will fulfil the Council's duties under the General Data Protection Regulations and the Data Protection Act 2018.	Corporate Insight, Communities and

		Governance Manager
Equalities	The recommendations do not propose a change in service therefore will not require an equalities impact assessment.	Corporate Insight, Communities and Governance Manager
Public Health	We recognise that the recommendations will not negatively impact on population health or that of individuals.	Corporate Insight, Communities and Governance Manager
Crime and Disorder	No Impact	Corporate Insight, Communities and Governance Manager
Procurement	No Impact	Corporate Insight, Communities and Governance Manager
Biodiversity and Climate Change	The implications of this report on biodiversity and climate change have been considered and are; There are no implications on biodiversity and climate change.	Corporate Insight, Communities and Governance Manager

2. INTRODUCTION AND BACKGROUND

2.1 The purpose of this report is to provide an update on the progress of compliance with the Data Protection Act 2018 (the General Data Protection Regulation (GDPR)) that became law on the 25 May 2018. A report was first presented in November 2017 which set out the proposed resources and actions required for compliance, alongside a detailed action plan. Members have been provided with an update at least once a year since.

2.2 The Council has worked proactively to improve how we manage and hold personal data in-line with the Data Protection Act. Whilst there have been additional burdens in terms of the work required to meet the Act the actions taken have improved how the Council operates and how we manage and use personal data. Colleagues across the Council have been receptive to change and training to increase understanding and awareness of data protection and effective data management across the Council. This report

provides an update on key changes and points of note, progress against the action plan and highlights the areas where further work is required.

3. Information of note

Consultation on changes to data protection legislation

3.1 The Department for Digital, Culture, Media and Sport (DCMS) have published a consultation document entitled Data: A new direction. Their stated aim is to amend UK GDPR, DPA 2018 and PECR 2003, so that it aligns with ambitions around growth and innovation and becomes easier to understand and work within the legislation. Consultation on the new proposals is open until the 19 November 2021.

3.2 A copy of the full consultation can be found at https://www.gov.uk/government/consultations/data-a-new-direction and an overview of the key proposals has been provided at appendix A. The most relevant chapters to the Council are chapters two, four and five. Proposals key to note are

- Replacing requirements around the accountability framework with a risk-based approach such as Privacy Management Programmes;
- Changes to reduce the burdens of DPIAs and breach reporting but replacing with voluntary undertakings processes;
- Introducing a fee for Subject Access Requests and introducing a threshold for cost for responding similar to FOIs;
- Removing the role of DPO but still retaining requirements for clear roles and responsibilities; and
- A robust complaints process to handle Data Protection complaints.

3.3 A response to the consultation is being proposed by the Council in response to those elements of chapters two, four and five which relate strictly to the Council. Overall, the changes do not raise a great deal of concern excluding the charge for Subject Access Requests, where it is noted that this may exclude those who are financially insecure. The proposals suggest a reduction in burdens which is welcome however, it is not considered that the changes proposed, as they relate the Council, will significantly reduce the burden of Data Protection.

Data sharing code of practice

3.4 The Information Commissioners Office has published its long-awaited code of practice for data sharing https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice/ The Code focuses on sharing of personal data between controllers. It does not cover sharing data with a processor (which should be subject to a data processing agreement) or within an organisation. It covers both routine/systematic data sharing and exceptional, one-off data sharing projects, as well as data pooling.

3.5 It does not impose any additional barriers to data sharing but provides practical advice on how to share data fairly and lawfully, as well as the best way to meet obligations of accountability. The code contains optional 'good

practice' recommendations and a necessary framework for negotiating information sharing which can be extremely challenging.

3.6 Learning from the code of practice will be rolled out to officers as part of data privacy week in January, information management training in early 2022 and existing training provided by the Data Protection Officer.

Information Commissioner's Office applies powers

3.7 Part of the ICO's role is to take action against those who don't meet their obligations in relation to data protection. In cases where a clear and serious breach of the legislation has taken place, the ICO will investigate and provide advice and instruction to help ensure the organisation gets it right in future. If an organisation isn't taking its responsibilities seriously, they may also take enforcement action. In the most serious cases, serving a monetary penalty of up to £17.5 million, or 4% of the total worldwide annual turnover, whichever is higher.

3.8 Reviewing relevant cases can be extremely helpful in providing real life cases of where things can go wrong to learn from and prevent similar cases occurring in the Council.

Direct Action against individuals

3.9 A motor industry employee unlawfully compiled lists of road traffic accident data including partial names, mobile phone numbers and registration numbers, transferring the data obtained to the director of an accident claims management firm. The two parties were ordered to carry out 100 hours' unpaid work and contribute £1,000 costs. A Confiscation Order, under the Proceeds of Crimes Act, to recover benefit obtained because of the offending had been given by the Court in which one party must pay £25,000 and the other £15,000 or face 3 months imprisonment.

Mermaids Charity

3.10 A charity set up an internal email group which was created with insufficiently secure settings, leading to approximately 780 pages of confidential emails to be viewable online for nearly three years. This led to personal information, such as names and email addresses, of 550 people being searchable online. The personal data of 24 of those people was sensitive as it revealed how the person was coping and feeling, with a further 15 classified as special category data as mental and physical health and sexual orientation were exposed. The charity was given a monetary penalty of £25,000.

HIV Scotland

3.11 The charity breached data protection through an email to 105 people which included patient advocates representing people living in Scotland with HIV. All the email addresses were visible to all recipients, and 65 of the addresses identified people by name. From the personal data disclosed, an assumption could be made about individuals' HIV status or risk. Whilst the charity acknowledged weaknesses in their approach, they continued to use

the same approach after the breach for a considerable time. The charity was given a monetary penalty of £10,000.

4. Progress against action plan and Next steps

4.1 The team set an ambitious action plan last year which was mainly focused on renewing existing documentation that had been put in place in advance of the DPA18. Large projects such as the programme of audits which were planned for summer 2021 have been postponed as they have not been possible to achieve alongside day-to-day data protection activities such as developing information sharing agreements and Data Protection Impact Assessments, which take up a substantial amount of the team's time.

4.2 Partly as a result of this there has been a change of structure this year within the Corporate Insight, Communities and Governance Team within whose remit data protection sits. The changes, which the service have made within existing budgets, were made with a focus on ensuring sufficient resources and resilience to information management activities across the Council. The Information Governance function is responsible for data protection, complaints, FOI/EIR and MP Correspondence, the structure of the Information Governance function can be seen at Appendix B. The changes have created a specific post to undertake the administrative elements of the service, allowing the Information Governance Officer greater capacity to focus on providing more day-to-day expert support to services, as well as a senior to share responsibility with the Corporate Insight Communities and Governance Manager for working with services to ensure that projects are compliant with legislation and information management is embedded.

4.3 The new Senior Information Governance Officer starts in January 2022 and the action plan has been re-timetabled to fit in with this, and delivery will be part of their objectives.

4.4 There have been a number actions successfully implemented

- Policies drafted;
- Updates made to Privacy notices;
- The CCTV review has been completed;
- Operational guidance and procedures have been updated;
- Issues with the Data Protection pages have been amended;
- A dashboard has been created which allows for the ongoing monitoring of performance of DPIAs, Subject Access Requests and Information Sharing;
- Operational Data Protection Meetings have been introduced and are minuted; and
- A range of training has been planned for the year, including FOI and specialist information sharing training, in addition to e-learning and tailored team meeting training provided by the Data Protection Officer and Deputy. Recent sessions have included HR, Housing and Environmental Services.

4.5 Currently the team are exploring systems which may reduce administrative burdens whilst at the same time ensuring accountability and reducing risk, these benefits will of course need to be balanced against cost. Work is

beginning on implementing CCTV actions as well as looking at redesign of privacy notices.

4.6 The 28 January 2022 is Data Privacy Day, and the Information Management Board has agreed a suggestion to run a week of activities to provide information and reminders on Data Protection. This is something that Members may also want to be involved in as they are data controllers in their own right.

4.7 Looking forward consideration could be given to the inclusion in this report of performance data relating to wider information management relating to

- The processing of requests under Freedom of Information Act /Environmental Impact Regulations;
- The processing of Subject Access Requests;
- Management of Data Breaches
- Information sharing Arrangements; and
- Data Protection Impact Assessments.

4.8 This would give a more complete view of the work going on in this area as well as the success of actions implemented to ensure compliance.

---

5. AVAILABLE OPTIONS

5.1 That the Audit, Governance and Standards Committee continues to receive an annual update on the progress of embedding GDPR into the Council's processes. The committee could choose to receive reports on specific areas of GDPR instead of an annual update. The Committee could choose not to receive any further updates on the delivery of the GDPR action plan

---

6. PREFERRED OPTION AND REASONS FOR RECOMMENDATIONS

6.1 That the committee continues to receive an annual update on the progress of embedding GDPR into the Council's processes until all actions become business as usual.

---

7. RISK

7.1 Accountability supports organisations to minimise the risk to personal data held, by putting in place appropriate and effective policies, procedures and measures. These must be proportionate to the risks, which can vary depending on the amount of data being handled or transferred, its sensitivity and the technology used.

---

8. CONSULTATION RESULTS AND PREVIOUS COMMITTEE FEEDBACK

8.1 The Committee has received a regular update since 2017. The chair of the committee also holds a place on the Council's Information Management Group.

9. REPORT APPENDICES

The following documents are to be published with this report and form part of the report:

- Appendix A: Consultation Data: A New Direction
- Appendix B: Information Governance Service Structure
- Appendix C: Action Plan