Audit, Governance and Standards Committee	**16 November 2020**

Data Protection Action Plan – Progress Update

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

Executive Summary

The Data Protection Act 2018 became law in May 2018. An action plan has been in place since 2017 to ensure the Council was prepared for the changes and to ensure it maintains compliant. This report provides an update on progress and sets out further actions required.

Purpose of Report

Noting

This report makes the following recommendations to this Committee:

1. To note national context and progress to date.
2. To note next steps and new action plan.

Timetable	
Meeting	***Date***
Corporate Leadership Team	3 November 2020
Audit, Governance and Standards Committee	16 November 2020

Data Protection Action Plan – Progress Update

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.	Policy and Information 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.	Policy and Information 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.	Policy and Information Manager
Financial	The proposals set out in the recommendation are all within already approved budgetary headings and so need no new funding for implementation.	Policy and Information Manager
Staffing	We will deliver the recommendations with our current staffing.	Policy and Information 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.	Policy and Information Manager
Equalities	The recommendations do not propose a change in service therefore will not require an equalities impact assessment.	Policy & Information Manager
Public Health	We recognise that the recommendations will not negatively impact on population health or that of individuals.	Public Health Officer
Crime and Disorder	No Impact	Policy & Information Manager

Procurement	No Impact	Policy & Information Manager

1. INTRODUCTION AND BACKGROUND

1.1. 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.

1.2. 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.

1.3. 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.

1.4. 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.

2. Information of note

<u>Exiting the EU</u>

2.1. When the UK leaves the EU, the Government has passed legislation so that personal data can continue to be processed between the UK and the EEA. However the UK is seeking adequacy decisions from the EU under both the General Data Protection Regulation and the Law Enforcement Directive (LED) which, if secured by the end of the EU Exit transition period on 31st December 2020, will allow for the free flow of personal data between the UK and the EU/EEA to continue uninterrupted.

2.2. The EU uses adequacy decisions to recognise that a country has data protection standards which are "essentially equivalent" to those in the EU, so there are no restrictions on transfers of personal data from the EU to that country, and no need for organisations to put in place any further arrangements to transfer data to organisations in that country.

2.3. On the 1st January 2021, at the end of the transition period, if no alternative agreement is in place, the UK will not retain its adequacy status and will become a 'third country' for data protection purposes. In the event that the European Commission have not recognised the UK as adequate by

the end of the transition period, transfer of personal data from the EEA to the UK will be restricted unless appropriate safeguards are in place, or the transfer benefits from one of the statutory exceptions.

2.4. Whilst it may seem that the Council would not process data from the EEA or send information to be processed by the EEA, processing includes the systems which are used for processing purposes and this means identifying whether 'cloud' or host supplier arrangements, including back-up facilities, may fall under this data flow category.

2.5. The Council has received guidance from MHCLG, for preparing for data protection after the EU Exit transition period ends. It recommends 3 key actions to be undertaken before 31 December 2020:

- Conduct an audit of personal data processing in your organisation, where the data is received from or sent to a third party.
- Identify your data flows from the EU/ EEA to the UK, and where you need to put in place alternative arrangements to allow data flows to continue in a 'no adequacy' scenario, take appropriate action.
- Identify data stored by EEA processors, for example cloud storage providers based in the EU and take appropriate action.

2.6. A majority of this work was completed at the end of 2019 and the beginning of 2020, and no major risks were identified. There are a couple of areas where further work is still required to ensure that systems are solely based in the UK and this is currently underway.

Information Commissioner's Office applying powers

2.7. At the Committee meeting in January 2020, members were circulated information on the first action taken by The Information Commissioner's Office (ICO) for breaches of the Data Protection Act 2018/General Data Protection Regulations.

2.8. Since then the ICO has also fined British Airways £20m for failing to protect the personal and financial details of more than 400,000 of its customers, after a cyber-attack.

2.9. An enforcement notice has also been served on Experian to make fundamental changes to how it handles people's personal data. It was identified that significant 'invisible' processing was being undertaken, likely affecting millions of adults. It is 'invisible' because the individual is not aware that the organisation is collecting and using their personal data.

The ICO's Accountability Framework

2.10. Accountability is one of the key principles in data protection. It requires that you comply and are able to demonstrate your compliance with the legislation.

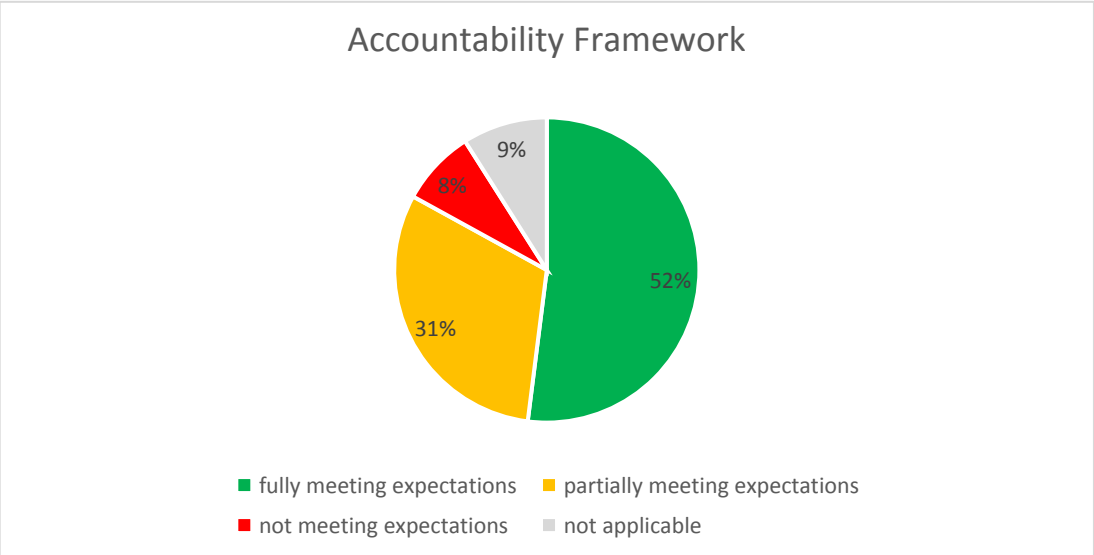
2.11. Accountability supports organisations to minimise the risk to personal data held, by putting in place appropriate and effective policies, procedures and measures. These must be proportionate to the risks, which can vary

depending on the amount of data being handled or transferred, its sensitivity and the technology used.

2.12. The ICO have produced a framework including an 'accountability tracker' to enable organisations to review their own arrangements and create plans to improve.

2.13. The Framework has ten themes, with a range of actions which an organisation complying with accountability and demonstrating best practice will demonstrate. When completing the self-assessment, the organisation will rank itself as, fully meeting, partially meeting or not meeting expectations.

2.14. A self-assessment of Maidstone's arrangements and compliance has been undertaken. A cautious and risk averse approach was taken to scoring, as the self-assessment is for the authority's benefit to identify areas of improvement. Maidstone's overall scores, and summary of performance across the areas can be seen below.



Accountability Framework Theme	Score - fully meeting expectations	Areas for improvement
The organisation has good leadership in place, making sure that staff have clear responsibilities for data protection-related activities at a strategic and operational level.	83%	Resources in place and documented roles and responsibilities.

Accountability Framework Theme	Score - fully meeting expectations	Areas for improvement
The organisation has policies and procedures providing clarity and consistency, by communicating what people need to do and why.	41%	Existing policies and procedures need updating, and should be consistent in style.
The organisation makes sure that all employees receive appropriate training about your privacy programme, including what its goals are, what it requires people to do and what responsibilities they have.	62%	New training programme needs to be developed and needs to cover different learning styles.
The organisation facilitates requests around individual's rights effectively.	76%	Clearer processes and procedures need to be in place to document decision making.
The Organisation has a 'data protection by design and by default' approach and this is documented by clear transparent privacy notices and staff awareness.	26%	Privacy Notice and statements need to be updated and a clear procedure and record keeping need to be in place to document privacy notice development moving forward.
It's a legal requirement for an organisation to document processing activities. Taking stock of what information is held, where it is and how it is processed.	35%	The Record of Processing Activity (ROPA) has recently been reviewed but changes need to implemented and a regular review needs to be recorded.

Accountability Framework Theme	Score - fully meeting expectations	Areas for improvement
It is good practice for to have written data sharing agreements when controllers share personal data. Written contracts help controllers and processors to demonstrate compliance and understand their obligations, responsibilities and liabilities.	67%	Some work is required to ensure Data Protection is embedded in the Procurement process, clearly.
The organisation identifies, assesses and manages privacy risks.	45%	An information Risk Policy and register is required. Information Risk needs to be included in more processes.
The organisation has good records management, it has good information access and has a good understanding of records processing	60%	Clearer processes to be implemented around use of social media and logs of system access to be as well documented and controlled as within ICT.
The organisation is able to detect, investigate, risk-assess and record any breaches. It has effective processes in place to decide when to report them as appropriate.	53%	Information on data protection needs to be more readily available for residents. Performance measures need to be put in place that are monitored regularly.

2.15. A majority of the actions are either in place or partially in place. Those that are partially in place may need updating, formalising, or expanding to meet the ICO's expectations.

2.16. The lowest scoring area is focussed on privacy notices and information, how we inform people we are using their data. We are fully or partially

meeting the majority of requirements, only 4 actions are red and these have been picked up in the action plan.

2.17. Overall only 9% of actions do not meet expectations, this equates to 28 actions. None of these are high risk areas, which should be cause for alarm and can mitigated. The only area which has limited mitigation is

Your organisation can deal with any increase in requests or reduction in staffing levels.

2.18. Resources are already limited on Data Protection. Over the next year, more of the Policy and Information and Executive Support teams will receive training on some aspects of Data Protection (e.g. redaction, rights requests) to provide some resilience but day to day resource is limited.

2.19. The self-assessment has been used to inform the updating of the new action plan which can be seen at appendix 1.

3. Progress to date and New Action Plan

3.1. There were three key areas discussed at the Committee meeting as being outstanding

- Updating of the Asset Register
- Implementing of actions from the CCTV review when it was completed
- Implementing actions from the Record of Processing Activity (ROPA) review when it was completed.

3.2. The ROPA and CCTV review completed in February. Due to the pandemic progress on remaining actions were paused. Resources in the Policy and Information Team were redeployed to support in a number of areas, over the lockdown period, and work on Data Protection has mainly focused on ensuing that necessary actions taken to respond to the health crisis were secure and appropriate.

3.3. Actions following the CCTV review have continued all be it slowly and policies have been developed and are in draft.

3.4. The new action plan can be seen at appendix 1. The new action plan incorporates those areas outstanding from the old action plan and those areas identified from the accountability self-assessment as not or partially meeting expectations. It also includes the remaining work to ensure compliance should the UK not receive adequacy status when it exits the EU.

3.5. The action plan is substantial and resembles the size of the action plan that the Council had when first implementing actions in preparation for GDPR in 2017. This is not to say the same work is required whereas the original action plan was focussed on compliance, this action plan is more detailed and focusses on best practice and information management in the round not Data Protection singularly.

3.6. The action plan covers the next 15 months. The next six to nine months will be focussed on

- Ensuring compliance for Exiting the EU
- Updating existing policies to ensure they are in line with best practice and new guidance
- Developing a new training programme which is appropriate to different roles within the organisation
- Implementing a new programme of Information Audits to develop information asset registers, and ensure services have appropriate processes in place.
- Ensuring Information Risk is appropriately managed.

3.7. Delivery of the action plan will be overseen by the Information Management Board.

---

4. AVAILABLE OPTIONS

4.1 The committee continues to receive an annual update on the progress of embedding GDPR into the Council's processes.

4.2 The committee could choose to receive reports on specific areas of GDPR instead of an annual update.

4.3 The Committee could choose not to receive any further updates on the delivery of the GDPR action plan.

---

5. PREFERRED OPTION AND REASONS FOR RECOMMENDATIONS

5.1 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.

---

6. RISK

6.1 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.

7. CONSULTATION RESULTS AND PREVIOUS COMMITTEE FEEDBACK

7.1 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, which oversees the GDPR action plan.

---

8. REPORT APPENDICES

- DPA Action Plan 2020/21