# Audit and Standards Committee Report

| | |
|---|---|
| **Report of:** | **Executive Director of Resources** |
| **Date:** | **20 September 2018** |
| **Subject:** | **Data Protection – General Data Protection Regulations Compliance Update** |
| **Author of Report:** | **Mark Jones**<br>**Data Protection Officer / Senior Information Management Officer** |

**Summary:**

To provide an update to the Council's position in preparing for and complying with the General Data Protection Regulations and the Data Protection Act 2018, both of which came into effect on May 25th 2018, the latter replacing the Data Protection Act 1998.

**Recommendations:** To note the actions to date and support the ongoing work.

**Background Papers:** Audit Committee Reports: 27 April 2017, 11 January 2018

**Category of Report:** OPEN

## Statutory and Council Policy Checklist

| |
|---|
| **Financial Implications** |
| NO: |
| **Legal Implications** |
| YES |
| **Equality of Opportunity Implications** |
| NO |
| **Tackling Health Inequalities Implications** |
| NO |
| **Human rights Implications** |
| NO: |
| **Environmental and Sustainability implications** |
| NO |
| **Economic impact** |
| NO |
| **Community safety implications** |
| NO |
| **Human resources implications** |
| NO |
| **Property implications** |
| NO |
| **Area(s) affected** |
| None |
| **Relevant Cabinet Portfolio Member** |
| Councillor Olivia Blake, Cabinet Member for Finance |
| **Is the item a matter which is reserved for approval by the City Council?** |
| NO |
| **Press release** |
| NO |

**Data Protection – General Data Protection Regulations Compliance Update**

## 1.0 INTRODUCTION

1.1 This report is an update to the work carried out within the Council to help prepare for and comply with the new data protection legislation that came into effect on May 25th 2018.

1.2 This report follows the two previous reports presented to the Audit and Standards Committee about the General Data Protection Regulations (GDPR) and the actions taken (27th April 2017 and 11th January 2018 respectively).

## 2.0 BACKGROUND

2.1 The GDPR came into effect In May 2018 with the aim to bring data privacy legislation up to speed with globalisation and technological advancements; and have a coherent approach to data privacy within Europe with all EU Member States following the same rules.

2.2 The Data Protection Act 2018 also came into effect on May 25th 2018, so that UK law would align with GDPR and replace the Data Protection Act 1998.

2.3 In 2017, the Head of Information Management set up a project team, with representatives from each portfolio, to work together to identify the work needed to comply with the new data protection requirements. This work included:

1. **Discovery** to identify the business activities that process personal data and to gather information to determine if the processing complies with the GDPR requirements. The scope of the discovery focused primarily on the activities processing large amounts of personal data or where the processing was considered to be high risk (e.g. confidentiality) and resulted in the creation of the Record of Processing Activity.

2. **Awareness** amongst our staff, third party contractors and processors that data protection was changing to help ensure they understand their obligations and take the necessary actions to comply with the law and to be able to demonstrate that compliance. This has been carried out in a number of ways including through data protection drop in sessions and training workshops; briefings, newsletters and updates; e-learning and supporting literature.

3. **Gap Analysis** between the Council's current practice and the data protection requirements identified where work was required. The

GDPR and supporting guidance from the EU's Article 29 Working Party provided a steer to what work was needed, but the Council (and other UK organisations) also needed the Data Protection Act 2018 to make clear any additional requirements or differences from GDPR. The Information Commissioner's Office has and continues to produce this guidance, which the Council uses to develop and implement best practice. An update of the actions taken is covered in Section 3.

## 3.0 MAIN BODY OF THE REPORT

Including Legal, Financial and all other relevant implications (if any)

3.1 The table below lists the main actions that were identified during the project and work taken to date:

| Area | Main actions identified | Status - January | Update - September |
|---|---|---|---|
| Consent | Only use when there is no legal power/ statutory duty available. This is in line with the Information Commissioner's Office advice.<br><br>Update communications in line to the Act so that when consent is used it's clear to the person consenting what they are consenting too, and includes for example the ability to opt out at any time.<br><br>Ensure that only "Opt In" is adopted when consent is required and that when consent has been provided it is through an affirmed action. | As part of stage one the council assessed where we have asked individuals for their consent to use their personal data.<br><br>From January onwards we intend to update communications and guidance so that when Consent is required it adheres to the requirements of the new legislation. | Completed.<br><br>Workshops and guidance provided to officers up until July 2018 to help distinguish the difference between consent and fair processing.<br><br>Consent is not the preferred legal basis to process personal data, but where it is necessary, it will be an affirmative and transparent action. |
| Subject | Update | Communications | Completed. |

| | | | |
|---|---|---|---|
| Access Requests (request for personal data) | communications and Standard Operating Procedures (SOP) to reflect changes, e.g. statutory period to complete a Subject Access Request.<br><br>Ability to provide that request electronically to the customer. | and operational guidance will be updated as part of stage 3. | SAR - Standard Operating Procedure updated and continuously reviewed to improve performance.<br><br>NB. SAR performance is lower than the Council's target and additional resources are being committed to resolve the issue |
| Retention | Embed existing retention periods into working procedures for paper and electronic information.<br><br>Raise awareness and update schedules within existing retention policy.<br><br>Commence further work around Records Management to support access and retrieval and disposal (paper and electronic information). | Some initial work has already taken place regarding our existing retention policies.<br><br>Further work will continue as part of stage 3. | In progress.<br><br>Retention Schedule currently being collated and will be validated by Portfolio Services.<br><br>Schedule to be published on the Council's web site by December 2018.<br><br>BCIS commissioned a review of the current records management position, which has consulted with officers across the Council, to determine the key challenges. |

| | | | |
|---|---|---|---|
| | | | Findings will inform the Information Management Strategy |
| Contracts | Review and update existing contracts where personal data is processed / shared.<br><br>Adopt when available Crown Commercial Services terms and conditions to new contracts. | Commercial Services informed existing suppliers of the changes in Data Protection legislation.<br><br>Within Stage 3 changes in contracts will be put into place where required. | In progress.<br><br>Model contract updated to include data protection references.<br><br>Letter of contract variation issued and contracts updated.<br><br>Work ongoing to ensure all new and existing contracts comply. |
| Privacy Notices | Review and update privacy notices so that they are in line with the requirements of the new Data Protection legislation.<br><br>Update the Councils main privacy notice and adopt a tiered approach to privacy notices, as outlined by the Information Commissioners Office. | We have assessed some existing privacy notices and rewritten some initial guidance based on ICO guidance.<br><br>Workshops are planned in January and February with staff that may need to rewrite privacy notices. | In progress.<br><br>Workshop training provided and well attended.<br><br>Privacy notice guidance and template produced for officers to use.<br><br>Privacy notices in place e.g. application forms, call centre voice recordings, website.<br><br>To publish the key privacy notices onto the Council's |

| | | | |
|---|---|---|---|
| | | | web site by the end of September 2019. |
| Capability of IT system/ technical and non-technical controls. | Ensure that technology used can delete and manage records in line with retention/ consider workarounds where there is no alternative.<br><br>Ensure that appropriate controls (technical and non-technical) are in place to safeguard personal data. | An initial assessment was undertaken in stage one.<br><br>We aim to address any necessary changes through contractual changes so that any new requirements are detailed appropriately. | In progress.<br><br>IT Applications are being assessed as part of the IT Strategy (Tech2020), which will identify applications that do not or cannot delete personal. |
| Information Governance Policies and Procedures/ Dashboard | Refresh existing Information Governance policies and procedures in line.<br><br>Development of a dashboard to support reporting on compliance to the Act that aligns to risk management reporting.<br><br>Create new Information Governance polices that will support the accountability principle of the Data Protection Act. | This will be developed in stage 3. | In progress.<br><br>Documents and Records Management Policy rewritten in Jan 2018.<br><br>Data Protection Policy rewritten to line with GDPR;<br><br>ICT Acceptable Use Policy under review to be replaced by new Information Security Policy.<br><br>Both policies to be reviewed by HR and Trade Unions |
| Data Protection Officer (DPO) | Ensure that reporting from the DPO is embedded into existing risk | Discussions have already taken place with Internal audit and | In progress.<br><br>Data Protection Impact |

| | | | |
|---|---|---|---|
| | management audit and annual governance procedures.<br><br>This includes the council's Annual Governance Statement.<br><br>Ensure that Data Privacy Impact Assessments are signed off and the necessary controls in place. | legal to ensure that any reports from the DPO align to existing risk management procedures.<br><br>Report produced by April detailing the responsibilities of the DPO and overall governance. | Assessments guidance and template in place referring to Data Protection Office role.<br><br>DPIAs to form part of business change and project governance and Annual Governance Statement |
| Accountability | Ensure sufficient evidence is created to demonstrate compliance with data protection. | To be covered in stage 3 – implement changes and review | In progress.<br><br>Record of Processing Activity (ROPA) has been created from the initial discovery survey identifying key business activities and the types of data being processed, which provides the means to document compliance with data protection.<br><br>The ROPA includes data fields for: legal basis, privacy notices, data protection impact assessments, information sharing agreements, retention, which are also key |

| | | | |
|---|---|---|---|
| | | | features measured as part of the Annual Governance Statement. |

3.2 As shown above, compliance to GDPR and data protection is an ongoing activity, so the GDPR project and working party finished in July and the work to develop and maintain compliance moved to the Information Governance Working Group to be part of business as usual.

3.3 As part of the above transition, the GDPR project plan has been updated to set out the tasks and activities that are still required. This action plan will be used by the Information Governance Working Group representatives to work within their respective portfolios to ensure data protection is embedded into working practice, which can be monitored and measured with the Annual Governance Statement.

## 4.0 RECOMMENDATIONS

4.1 To note the actions to date and support the ongoing work.

This page is intentionally left blank