



## Audit and Standards

---

**Report of:** Executive Director, Resources

---

**Date:** 11 January 2018

---

**Subject:**

UPDATE ON WORK UNDERTAKEN AND FUTURE WORK PLANNED TO ADDRESS THE REQUIREMENTS OF THE DATA PROTECTION ACT 2018.

---

**Author of Report:** JOHN L CURTIS, HEAD OF INFORMATION MANAGEMENT, INFORMATION MANAGEMENT, BUSINESS CHANGE AND INFORMATION SOLUTIONS, RESOURCES

---

**Summary:**

This report provides an update on work undertaken and planned to address the requirements of the forthcoming Data Protection Act 2018 which will be introduced on the 25<sup>th</sup> May 2018.

---

**Recommendations:**

To note and continue to support the ongoing work.

---

**Background Papers:**

Reference should be made to the internet links detailed within the report, and initial paper presented to the Audit Committee on 27<sup>th</sup> April 2017.

---

**Category of Report:** OPEN

## Statutory and Council Policy Checklist

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

## **UPDATE ON WORK UNDERTAKEN AND FUTURE WORK PLANNED TO ADDRESS THE REQUIREMENTS OF THE DATA PROTECTION ACT 2018.**

### **1. INTRODUCTION**

- 1.1.** This report provides a further update on the project to meet the requirements of the forthcoming Data Protection Act 2018. This comes into force on the 25th May 2018.
- 1.2.** The Data Protection Act 2018 will replace the existing Data Protection Act 1998 and will ensure that the United Kingdom meets the legal requirements of the EU General Data Protection Regulation (GDPR).
- 1.3.** Further information about this project and proposed changes in legislation can be found within the initial report presented to the Audit Committee on 27 April 2017. A copy of this initial report can be found [here](#).

### **2. BACKGROUND**

- 2.1.** As outlined in the initial Audit Committee report on GDPR, the European Union Commission proposed a General Data Protection Regulation (GDPR) in 2012. This was to achieve the following objectives:
  - 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.** To meet the requirements of the GDPR, the United Kingdom has introduced the Data Protection Bill which is currently going through its parliamentary stages. Further information about the Data Protection Bill and its stages through parliament can be found [here](#).
- 2.3.** More details about the proposed changes in legislation can be found within the initial GDPR report Initial Report to the Audit Committee on GDPR.
- 2.4.** To address these changes the Council has put in place a project team. This project team includes membership from across the Council,

with support from Zurich, the Council's insurers. Their role is to quality assure the project from a risk management perspective.

### **3. PROJECT UPDATE AND STAGES OF THE PROJECT**

**3.1.** At high level, there are 3 key stages to the project. These stages are explained within this section and include a description of the work undertaken, findings and actions, as well as any work already completed or planned.

#### **3.2. Stage One - Discovery & Awareness**

3.2.1. This stage one was from April to December 2017 and has been completed. The purpose of this stage was to review and audit in more detail what personal data we collect and hold; the purpose(s) for that processing; the legislation allowing that processing and addressing other questions regarding consent and retention.

3.2.2. This information was collected through the distribution of two council-wide surveys to managers regarding personal data collected by that service area, as well as a further survey that was sent to IT system administrators regarding the technology used and its capability.

3.2.3. The project team initially received over 170 completed surveys regarding the processing of personal data and over 77 completed surveys in relation to IT systems used to process personal data. These surveys have been validated and have provided an insight into where work needs to be undertaken to address the changes in Data Protection legislation.

3.2.4. This stage also included raising awareness to all suppliers by making them aware of the changes in legislation which maybe applicable to the service they provide to the Council. It also outlined that where they are processing personal data on our behalf of the Council we will more than likely have to update existing contracts. This will take place in January 2018, and be an ongoing activity.

3.2.5. Raising staff awareness of the changes in legislation has been important. Staff have been updated through the managers brief; intranet communications, and a series of workshops, and weekly drop in clinics. The Council also intends to roll out and refresh Information Governance e-learning content, which includes a short engaging video explaining more about the Act and your role and responsibilities as a council employee.

3.2.6. The Councils Internet content has also been updated to inform the public of the work we are undertaking and what these changes mean for them. We also do intend to run some consultation forums with the public about how we use their data next year.

3.2.7. Within this phase, we have also updated our security/ data breach reporting process, which will support the mandatory timescale of reporting to the Information Commissioners Office (ICO) within 72 hours.

### **3.3. Stage Two – Gap Analysis**

3.3.1. This stage started in July and will continue into early 2018. This stage has partially run in parallel to stage one and has primarily consisted of reviewing the results from the two surveys and identifying what changes need to be made. It also includes completing where necessary Data Privacy Impact Assessments (DPIA) which assesses privacy, risks and controls that need to be in place to support fair, lawful and appropriate processing. The work around completing DPIA's will continue into stage three and be an ongoing activity.

3.3.2. The analysis undertaken within this stage has shown that further changes need to be made in particular which is detailed in table one. The areas of work primarily form activities within stage 3 of the project which commences in earnest in January 2018.

**Table One:** Some key changes that were identified as part of stage 2

<b>Area</b>	<b>Main actions identified</b>	<b>Status</b>
Consent	Only use when there is no legal power/ statutory duty available. This is in line	As part of stage one the council

	<p>with the Information Commissioner's Office advice.</p> <p>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.</p> <p>Ensure that only "Opt In" is adopted when consent is required and that when consent has been provided it is through an affirmed action.</p>	<p>assessed where we have asked individuals for their consent to use their personal data.</p> <p>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.</p>
Subject Access Requests (request for personal data)	<p>Update communications and Standard Operating Procedures (SOP) to reflect changes, e.g. statutory period to complete a Subject Access Request.</p> <p>Ability to provide that request electronically to the customer.</p>	<p>Communications and operational guidance will be updated as part of stage 3.</p>
Retention	<p>Embed existing retention periods into working procedures for paper and electronic information.</p> <p>Raise awareness and update schedules within existing retention policy.</p> <p>Commence further work around Records Management to support access and retrieval and disposal. (paper and electronic information).</p>	<p>Some initial work has already taken place regarding our existing retention policies.</p> <p>Further work will continue as part of stage 3.</p>
Contracts	<p>Review and update existing contracts where personal data is processed / shared.</p> <p>Adopt when available Crown Commercial Services terms and conditions to new contracts.</p>	<p>Commercial Services informed existing suppliers of the changes in Data Protection legislation.</p> <p>Within Stage 3 changes in</p>

		contracts will be put into place where required.
Privacy Notices	<p>Review and update privacy notices so that they are in line with the requirements of the new Data Protection legislation.</p> <p>Update the Councils main privacy notice and adopt a tiered approach to privacy notices, as outlined by the Information Commissioners Office.</p>	<p>We have assessed some existing privacy notices and rewritten some initial guidance based on ICO guidance.</p> <p>Workshops are planned in January and February with staff that may need to rewrite privacy notices.</p>
Capability of IT system/ technical and non-technical controls.	<p>Ensure that technology used can delete and manage records in line with retention/ consider workarounds where there is no alternative.</p> <p>Ensure that appropriate controls (technical and non- technical) are in place to safeguard personal data.</p>	<p>An initial assessment was undertaken in stage one.</p> <p>We aim to address any necessary changes through contractual changes so that any new requirements are detailed appropriately.</p>
Information Governance Policies and Procedures/ Dashboard	<p>Refresh existing Information Governance policies and procedures in line.</p> <p>Development of a dashboard to support reporting on compliance to the Act that aligns to risk management reporting.</p> <p>Create new Information Governance policies that will support the accountability principle of the Data Protection Act.</p>	<p>This will be developed in stage 3.</p>
Data Protection	<p>Ensure that reporting from the DPO is embedded into existing risk</p>	<p>Discussions have already taken</p>

Officer (DPO)	<p>management audit and annual governance procedures. This includes the councils Annual Governance Statement.</p> <p>Ensure that Data Privacy Impact Assessments are signed off and the necessary controls in place.</p>	<p>place with Internal audit and legal to ensure that any reports from the DPO align to existing risk management procedures.</p> <p>Report produced by April detailing the responsibilities of the DPO and overall governance.</p>
---------------	--	--

### 3.4. Stage Three – Implement Changes and review

- 3.4.1. This stage will commence in earnest in January 2018 and will primarily focus on the actions in the previous section. Other related actions which are specific to processing personal data will become apparent through the completion of Data Privacy Impact Assessments (DPIA).
- 3.4.2. We will continue to monitor and report progress made to the Executive Management Team and Audit Committee and will report any risks/ issues associated with this project.
- 3.4.3. Currently the project is reporting an Amber status due to the project slipping by approximately four weeks, and the volume of work required.
- 3.4.4. It is important that the evidence base created to support this work is maintained and that overall we embed into working practices the new requirements of this legislation. This will support the new principle of accountability. We will ensure that ongoing work for this project is aligned to existing risk, audit and governance practices.
- 3.4.5. There will be a review of the work undertaken by the designated Data Protection Officer (DPO) in early April 2018 to ensure that, where required, further actions are undertaken to meet the



requirements of the Act. This will be reported to the Executive Management Team and where appropriate and requested Audit Committee.

This page is intentionally left blank