Portsmouth CITY COUNCIL

Title of meeting: Governance & Audit & Standards Committee

Date of meeting: 1 February 2019

Subject: General Data Protection Regulation Programme Report

Report by: Michael Lawther, City Solicitor/Senior Information Risk Owner

Wards affected: All

Key decision: No

Full Council decision: No

---

1. Purpose of report

To inform the Committee of the work already undertaken and ongoing to ensure the Council's compliance with the General Data Protection Regulations and Data Protection Act 2018.

2. Recommendations

It is recommended that Members of the Governance & Audit & Standards Committee note the actions taken.

3. Background

PCC was first made aware of the emerging requirements of the General Data Protection Regulations (GDPR), in January 2016. The Information Commissioners Office (ICO) continued to develop and define the impact on UK organisations throughout 2016 and PCC commissioned specific consultancy to assess its position. This review and scoping took place in January 2017 and defined what PCC needed to accomplish to meet the 25th May 2018 deadline when the GDPR and Data Protection Act 2018 came into force.

A corporate programme was established in May 2017 to define and manage the work streams required. The programme has been overseen by a Board headed by Michael Lawther as Senior Information Risk Officer (SIRO). Programme and Project management resource has been supplied by the IT Service Programme and Projects team and delivered according to the established delivery standards. The Board has met monthly to review progress, address issues and help mitigate risks with additional fortnightly meetings of the Project Team.

The identified workstreams were:-

1. **To carry out a corporate-wide data mapping exercise**
   This identified all of the Council's uses of personal data and actions required to ensure its lawful processing under the new Regulations. Actions included the

review and development of Privacy Notices, Contracts/Agreements, retention of records and system functionality. In parallel the IT Development team produced an Electronic Information Asset Register to hold the gathered data, allow updates and refinements as well as providing reporting functionality to enable the management of information assets going forward.

2. **To review all relevant policies and procedures to ensure they reflected the new requirements.**
   All policies and procedures involving the processing of personal data were identified and reviewed. Policy authors were provided with suggested wording to enable them to update the documents. Policies will continue to be regularly reviewed in line with Council requirements via PolicyHub.

3. **To raise staff awareness through Corporate Communications and sector specific groups.**
   Corporate messages (Intranet and email) were issued to all staff to raise awareness and the Corporate Information Governance team delivered bespoke sessions to individual teams including Councillors. A dedicated page of guidance was developed in Intranet including fact sheets and templates.

4. **To formulate and deliver specific GDPR related training.**
   A mandatory online training module was developed and rolled out to all staff and Councillors in February 2018. All managers were reminded to ensure staff completed the training by 25th May 2018, and further corporate messages re-enforced this to all staff. Completion of the module has been monitored on a monthly basis since then and reported to the GDPR Programme Board. Lists of staff not having completed the training have been provided to managers to facilitate follow-up. Compliance is currently at approximately 90% of all staff. It should be noted that the percentage of non-compliant staff includes those who are on maternity leave/long term sickness absence and those on the temporary employment register who are not currently engaged by the Council.

5. **To work with partners or organisations for whom the Council has some responsibility to ensure their compliance.**
   Members of the Project Team met with relevant groups (e.g. Schools, Solent Local Enterprise Partnership, Portsmouth International Port, PCMI, Gosport Borough Council) and mirrored the work being done across the Council to ensure their compliance.

Following the May 2018 launch of GDPR, IT Service has continued to provide programme management and oversight of the identified work streams and is working towards the transition to Business As Usual (BAU). Work has continued with the following streams:-

Training - (work-stream owned by the Corporate Information Governance Team) The module is under review and will be updated and rolled out again in early 2019. A bespoke online module has been developed for Councillors and is available now on the Portsmouth Learning Gateway. The Information Governance team will

continue to work with Corporate Communications to issue reminders to staff, monitor compliance rates and report to the Corporate Information Governance Panel going forward.

IT applications - (work-stream owned by the IT Service**)** The data mapping exercise prior to 25th May 2018 identified applications containing personal data and GDPR compliance works are underway with a number of applications. All works required to remaining applications are being reviewed, risk assessed and prioritised. Some compliance issues will be addressed by the planned replacement of applications with more up-to-date alternatives e.g. the migration from Swift AIS to SystmOne for Adult Social Care case management. The works required to meet GDPR compliance for all identified applications represents a significant investment of time and resources by PCC and in most cases is dependent on the supplier. In general 'works' will consist of a system upgrade which requires installation of a test system, technical/system testing, integration testing (links to other systems e.g. EBS/finance), user acceptance testing, training and launch. In the future, once the review of all the applications is complete this will be covered by the ongoing BAU activities for the applications

Contracts - (work-stream owned by Legal Service) The wording of all new contracts has been developed in accordance with ICO guidance to ensure suppliers' responsibilities under GDPR and DPA 2018 are accurately reflected going forward. Work to review existing contracts (strategic, operational, or transactional) has continued to ensure they are compliant. This is being achieved by issuing a Deed of Variation to the contracted party for signature and the relevant amendment being made to the contract. Work has been prioritized using a risk matrix. Advice is being sought from the ICO and industry peers to inform the adaption of the Council's existing contract monitoring process to ensure contractors are fulfilling their responsibilities under GDPR on an ongoing basis.

Information Asset Register and Information Asset Owners (work-stream owned jointly between IT and Corporate Information Governance) Reporting functionality and **c**onfiguration for administration and account access within the Electronic Information Asset Register has been developed and is being tested with users in early 2019. Once signed off, the Information Asset Owners and other nominated staff will be trained in the use of the application which will enable them to update/amend entries relating to their area of the business. A regular programme of updating the register will be rolled out.

The ICO continues to refine and develop guidance on GDPR and the Data Protection Act 2018 and PCC responds to these updates as and when they are issued. In addition PCC's Data Protection Officer and Information Security Officer are in regular contact with the ICO and industry peers as working practices are developed.

4. Reasons for recommendations

To ensure the Governance & Audit & Standards Committee has an oversight of the work completed.

5. Equality impact assessment

An equality impact assessment is not required as the recommendation does not have a negative impact on any of the protected characteristics as described in the Equality Act 2010.

6. Legal implications

The Council is required to ensure that it has robust procedures in place to comply with its obligations under the General Data Protection Regulation (GDPR) 2016. Bringing this report to the Committee's attention will assist in meeting those requirements.

7. Director of Finance's comments

The Programme Manager is working with IT officers to identify the cost implications of the GDPR compliance works associated with existing IT applications. Wherever possible expenditure will be met from within existing Portfolio Cash Limits however, any shortfall may become a call on the Councils contingency budget.

The ICO can issue fines of up to €20 million or 4% of the authority's annual turnover for serious breaches of the GDPR. Breach of the Privacy and Electronic Communications Regulations also incurs a financial penalty**.** The size of any monetary penalty is determined by the Commissioner taking into account the seriousness of the breach and other factors such as the size, financial and other resources of the data controller. Any breaches put the City Council at risk of the unbudgeted cost of a financial penalty which would have to be met from the service responsible for the breach.

……
Signed by:

Appendices: None

Background list of documents: Section 100D of the Local Government Act 1972

The following documents disclose facts or matters, which have been relied upon to a material extent by the author in preparing this report:

Title of document	Location
None	