Committee:	Dated:
Community and Children's Services Committee	14/09/2018
Subject: The General Data Protection Regulation	**Public**
Report of: Andrew Carter, Director of Community and Children's Services	**For Information**
Report author: Simon Cribbens, Assistant Director of Commissioning and Partnerships	

Summary

This report sets out activities undertaken by the Department of Community and Children's Services (DCCS) to ensure compliance with the General Data Protection Regulation (GDPR).

Recommendation

Members are asked to:

- Note the report.

Main Report

Background

1. The GDPR is based on a European Union directive to standardise data privacy laws across Europe. It came into effect on 25 May 2018 and applies to any organisation located within the EU that processes personal data. It substantially updates existing data protection law, setting out measures to:

    - ensure that personal data is used legitimately and fairly
    - provide greater protection and rights for individuals whose personal data is held
    - put in place accountability, governance and security protocols to safeguard data.

2. The GDPR has been introduced in response to significant changes to IT and ways that organisations now process and share data. It is a further compelling requirement when set against the backdrop of wider societal data security concerns and cyber resilience. It is enshrined in UK law through the Data Protection Act 2018.

3. In the DCCS and wider local government, use of personal data is increasingly relied on to inform service demand and strategic decision-making. The DCCS stores and processes significant personal data, much of it sensitive information

on vulnerable service users. Sharing data with partners and providing data to external organisations for analysis and storage is becoming a more common, business-as-usual requirement. It is highly likely that these practices will continue to increase in regularity and scale.

4. In Autumn 2017 the Comptroller's office set out a project plan to review the Corporation's information governance practices and policies and embed new GDPR protocols. This was to ensure that the necessary technical IT and information security systems are GDPR compliant.

5. A DCCS work programme was developed in line with the Comptroller's plan, with a focus on ensuring that all personal data sets held by the department are compliant with the GDPR.

6. A departmental audit of personal data sets was undertaken in December 2017 and provided a baseline to establish existing departmental compliance with the GDPR.

7. Using the outcomes of the audit, a gap analysis exercise was undertaken to establish non-compliance of personal data sets held across the department. This then informed unique action plans to ensure compliance across all DCCS divisions.

8. The Strategic Education division of the DCCS ran a seminar for the City of London (CoL) family of schools offering insight and guidance on the GDPR in an educational context. Guidance on data retention procedures has also been circulated to the CoL family of schools.

Activities undertaken to meet GDPR requirements

9. Appendix 1 sets out corporate and departmental activities to meet key requirements of the GDPR.

Current activities

10. A departmental lead officer has been nominated to ensure continued compliance with the GDPR. Key activities of this role are to:

    - delete personal data that is no longer needed, including data that has been archived

    - develop an updated departmental retention schedule

- maintain a schedule of ongoing compliance activities, including (but not limited to):
    - periodic review and update of the departmental Record of Processing Activities
    - periodic review of the retention schedule.

- finalise data-sharing agreements with Government departments to reflect the GDPR and Data Protection Act 2018 requirements
- finalise a departmental GDPR 'toolbox' for DCCS staff.

Conclusion

11. The GDPR substantially updates data protection law, including changing conditions for processing and strengthening privacy and other rights. The Comptroller's office and DCCS have delivered a programme of work to ensure that personal data sets held comply with GDPR requirements and that staff comply with policies that reflect the new ways of working.

Appendices

- Appendix 1 – Activities undertaken to meet GDPR requirements

Simon Cribbens
Assistant Director of Commissioning and Partnerships

T: 020 7332 1638
E: simon.cribbens@cityoflondon.gov.uk

Appendix 1 – Activities undertaken to meet GDPR requirements

Ensure that personal data is used legitimately and fairly	
GDPR requirement	**Departmental/corporate activity**
Ensuring a legal basis for processing personal data Local authorities now have more limited scope to rely on consent or legitimate interests and must have a valid lawful basis in order to process personal data, as below: i. **Consent –** the individual has given clear consent to process their personal data for a specific purpose ii. **Contract –** the processing is necessary for a contract with the individual, or because they have asked the CoL to take specific steps before entering into a contract iii. **Legal obligation –** the processing is necessary for the CoL to comply with the law (not including contractual obligations) iv. **Vital interests –** the processing is necessary to protect someone's life v. **Public task –** the processing is necessary for you to perform a task in the public interest or for the CoL's official functions, and the task or function has a clear basis in law vi. **Legitimate interests –**This basis cannot apply for public authority processing data to perform official tasks.	Following review and gap analysis, all personal data held across the department now complies with at least one lawful basis for processing personal data.
Review and implement new privacy notices The GDPR sets out greater emphasis on making privacy notices understandable and accessible. Information that needs to be provided when collecting personal data includes: The purposes for processing personal data; how long the data will be retained for; and who it might be shared with.	A corporate privacy notice template has been developed and circulated to all departments. It is set out on the CoL website at: www.cityoflondon.gov.uk/about-our-website/Pages/privacy-notice.aspx All DCCS divisions have identified requirements to amend or create new privacy notices specific to the requirements of the service provided. There are 20 DCCS privacy notices published on the CoL website at: www.cityoflondon.gov.uk/about-our-website/Documents/dccs-privacy-notice.pdf

Provide greater protection and rights for individuals whose personal data is held	
GDPR requirement	**Departmental/corporate activity**
Additional rights for individuals This requires new and updated Council procedures to respond to enhanced citizen rights, including the right: i. to be informed about the collection and use of their personal data ii. of access to their personal data and supplementary information iii. to rectification of inaccurate personal data iv. to erase personal data v. to restrict processing of personal data vi. to data portability, which allows individuals to obtain and reuse their personal data for their own purposes across different services vii. to object to processing viii. in relation to automated decision-making and profiling.	The Comptroller's office has developed a series of corporate policies that set out a commitment and procedures to meet all enhanced citizen rights. Also published is an overall Data Protection Policy at: www.cityoflondon.gov.uk/about-the-city/access-to-information/Documents/data-protection-policy.pdf The DCCS complies with the policies and procedures set out by the Comptroller.
Data Protection Impact Assessment (DPIA) A DPIA identifies and minimises a project's data protection risks. A DPIA is advisable for certain listed types of processing, or any other processing that is likely to result in a high risk to individuals' interests. The DPIA must: • describe the nature, scope, context and purposes of the processing • assess necessity, proportionality and compliance measures • identify and assess risks to individuals • identify any additional measures to mitigate those risks.	The DCCS worked with the Comptroller to design and pilot a DPIA that has now been rolled out across the Corporation for use by all departments.

Put in place accountability, governance and security protocols to safeguard data	
GDPR requirement	**Departmental/corporate activity**
Third-party contracts We will need to have contracts with bodies we share data with, and those that process data on our behalf. Whenever the Corporation uses a data processor it needs to have a written contract in place enabling both parties to understand their responsibilities and liabilities.	A standard contract template that sets out clauses to meet Corporation GDPR requirements was developed and circulated in March 2018. The Information Audit undertaken in December 2017 identified third parties that process personal data on behalf of DCCS. Contract amendments setting out an updated Data Protection Schedule have been circulated to all identified third parties.
Less time for Subject Access Requests (SARs) The time limit for responding to SARs will be reduced from 40 days to one month, and the information which must be provided will be extended.	The DCCS is compliant with new corporate procedures and guidance.
New breach notification rules Breaches will have to be notified to the Information Commissioner's Office (ICO) within 72 hours where feasible, unless the breach is unlikely to result in risk to individuals. Where a high risk to individuals arises the ICO will also have to be notified, unless an exception applies.	The DCCS will comply with procedures set out by the Comptroller, including use of a breach notification form.
Deliver staff GDPR training Training provided to raise awareness of changes to data protection law and set out responsibilities for CoL staff.	All staff completed online GDPR training. A bespoke training package has been developed for staff that have limited web and/or English language skills.
Increased enforcement powers Fines for breaches of the Data Protection Act 1998 were limited to £500,000. This will be increased to £10 million or 2% of annual turnover or £20 million or 4% of annual turnover, depending on the nature of the breach, with the latter applying to breaches of the data protection principles and data subject rights.	Comptroller to oversee measures to respond to data breaches and potential fines.

Appointment of a Data Protection Officer (DPO) All public authorities will have to appoint a DPO to: • provide information, training and advice about GDPR compliance and other data protection laws • monitor compliance with the GDPR and other data protection laws • be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers, and so on).	The Comptroller is the Corporation's data protection officer.
Record of Processing Activities (RoPA) A RoPA will need to be held by the Corporation. The information required includes the purposes of the processing, categories of data subjects, personal data, those to whom data will be disclosed, and the general technical and security measures in place.	DCCS have now completed the RoPA.