



Council
3 May 2018
GDPR update

Classification Public

Purpose For noting

Issue The paper presents an update on the approach to updating the GOsC Information Governance Framework to meet the new requirements of the General Data Protection Regulation (GDPR).

Recommendation To note the update on GDPR compliance.

Financial and resourcing implications No additional budget requirement identified.

Equality and diversity implications None identified.

Communications implications The Information Governance Framework is a public document published on the GOsC website.

Annexes None

Author Tim Walker

Background

1. Council received an update on preparations for compliance with the General Data Protection Regulation at its January 2018 meeting. At that meeting it was reported that WardHadaway had been engaged to work with the Executive team on a consultancy basis to assist with preparations.
2. This paper provides a further update on this preparatory work.

Discussion

3. WardHadaway undertook a comprehensive audit in December/January and provided a report identifying the compliance gaps and providing a route map with recommendations as to how those gaps can be closed.
4. Aspects of the report were very positive with the auditors stating that 'the GOsC's arrangements for data protection compliance with regard to governance and controls provide a reasonable assurance that processes and procedures are in place and being adhered to'. Nevertheless and as expected there are a number of areas where the need for improvements has been identified.
5. The issues identified were wide-ranging. Some of these related to key aspects of GDPR compliance, some to ensuring best practice in data protection, and others to consistent compliance with existing policies and procedures. They included:
 - a. Reviewing IT access rights to ensure consistency
 - b. Improving password and other electronic security, including those used for document transfers
 - c. Improving manual storage and classification of documents
 - d. Strengthening arrangements around equipment disposal
 - e. Reviewing and updating contracts
 - f. Clarifying arrangements for transferring any data outside the EEA
 - g. Improving training and awareness of staff
 - h. Updating policy documents
 - i. Reviewing privacy notices and consent forms.
6. The issues identified have now been mapped into a GDPR Action Plan which is being reviewed regularly by the Senior Management Team.
7. The priority actions within the Action Plan relate to formal GDPR compliance and these will be concluded before the GDPR implementation date of 25 May 2018. These include:
 - a. Drafting new general and specific privacy and related consent notices explaining what data we hold, for what purpose and how this may be shared.

- b. Reviewing contractual arrangements with third party suppliers where these involve the use of personal data (approximately ten suppliers), including where any processing takes place outside the EU.
 - c. Reviewing current agreements with non-executives who have access to personal data as part of their work for the GOsC.
 - d. Updating the Information Governance Framework and ensuring that specific policies are up to date, including those relating to data breaches and data retention.
8. The remainder of the Action Plan, including areas of best practice and training will be implemented as the year progresses.
9. The Executive has been reporting regularly to the Audit Committee on GDPR and other information governance issues and intends to update it on progress with implementation of the Action Plan.

Recommendation: to note the update on GDPR compliance.