ABERDEEN CITY COUNCIL

| | |
|---|---|
| COMMITTEE | Audit, Risk & Scrutiny |
| DATE | 26 September 2017 |
| REPORT TITLE | Information Governance Report & the General Data Protection Regulation |
| REPORT NUMBER | CG/17/109 |
| CG LEAD OFFICER | Fraser Bell |
| REPORT AUTHOR | Helen Cannings |

## 1. PURPOSE OF REPORT:-

To provide Committee with an annual report on the Council's Information Governance Performance, and information about the incoming General Data Protection Regulation, and the Council's readiness approach.

## 2. RECOMMENDATION(S)

It is recommended that committee:

i. Note the information provided about the Council's information governance performance at sections 3.1 – 3.6 and in the Information Governance Report at Appendix 1.

ii. Note the information about the General Data Protection Regulation (GDPR) and its anticipated impact on the Council at sections 3.7 – 3.11.

iii. Note the Council's GDPR readiness approach, as part of the Council's wider information assurance improvement plan at sections 3.12 – 3.14.

## 3. BACKGROUND

### Annual Information Governance Performance Report

3.1 The Council's Audit, Risk and Scrutiny Committee agreed the Council's revised and updated Information Governance Management & Reporting Framework in September 2016; as part of this the Committee agreed to receive an annual report in relation to the Council's information governance performance, this is the first of these reports.

3.2 Also as directed by Audit, Risk & Scrutiny Committee in September 2016, the Information Governance Group has implemented Quarterly Information Governance Reporting, which brings together performance information in

relation to freedom of information, data protection and information security. This report collates analyses and monitors the Council's performance in relation to compliance with information legislation, and information security, to ensure that trends, issues, incidents, and breaches are dealt with appropriately as they arise by the Information Governance Group.

3.3 Ensuring the proper use and governance of the Council's information and data is an ongoing activity. New and changing legislation, systems, staff, and ways of doing business, as well as new and emerging cyber threats all shape and change the environment within which the Council operates in relation to effective use and governance of its information and data.

3.4 Keeping up means a careful balancing between the requirement to monitor and be adaptable to our changing environment, and the requirement to agree and implement assurance improvements over the medium term.

3.5 For this reason, the Information Governance Group has established an Information Assurance Improvement Plan which will implement the required medium term assurance improvements required. Progress to date on this work has been included in the Annual Report on the Council's Information Governance Performance.

3.6 Please refer to **Appendix 1** for the consolidated Annual Report on the Council's Information Governance Performance from July 2016-June 2017.

**The General Data Protection Regulation**

3.7 The General Data Protection Regulation (GDPR) will come into force in the UK on 25 May 2018. The GDPR will have direct effect in the UK without the need for any national implementing legislation. This is the most significant change to privacy legislation since the Data Protection Act 1998 came into force, and will effect changes to the Council's compliance requirements.

3.8 The UK Information Commissioner's Office (the ICO), who regulate data protection compliance in the UK, have begun to issue guidance on GDPR, which emphasises the importance of a planned and proactive readiness approach to new GDPR requirements.

3.9 The aim of GDPR is to put individuals in control of their own personal data, and the way it is handled by organisations, and to harmonise data protection legislation across the European Union. GDPR brings in other requirements which will impact on the Council's governance arrangements for, and day to day management of, personal data.

3.10 These include the Accountability Principle which requires the Council to be able to proactively record and demonstrate how our business activities comply with GDPR; changes to the conditions the Council can rely on for processing personal data; new and strengthened rights for individuals; and the requirement to have a statutory Data Protection Officer.

3.11 The penalties for non-compliance will increase from the current maximum of £500,000, to a penalty of up to €20,000,000, or 4% of turnover, whichever is higher.

**Readiness Approach**

3.12 Readiness for GDPR is being managed as a key part of the Council's Information Assurance Improvement Plan for 2017-18, to make sure that the requirements of new regulation are understood and managed as part of our broader interrelated programme of work to manage and improve information assurance.

3.13 This programme is establishing the holistic, foundational people, policy, process and learning information assurance components which need to be in place for the Council to be ready for GDPR in May 2018. A key component of the approach will be the embedding of Information Asset Owner roles throughout the Council at a third tier level, who will be accountable for managing information assets under their stewardship in line with corporate standards, and providing regular assurance to the Council's Senior Information Risk Owner (the SIRO).

3.14 An update on progress with the Council's Information Assurance Improvement Plan has been included in the Annual Report at **Appendix 1**.

## 4. FINANCIAL IMPLICATIONS

There are no direct financial implications arising from this report. There are potential indirect financial implications related to penalties for non-compliance, as outlined at section 5.3, below.

## 5. LEGAL IMPLICATIONS

5.1 The Council's use and governance of its information is subject to a variety of legislation including: the Data Protection Act 1998, the General Data Protection Regulation (from 25 May 2018), the Public Records (Scotland) Act 2011, the Freedom of Information (Scotland) Act 2002, the Environmental Information (Scotland) Regulations 2004, and the Re-use of Public Sector Information Regulations 2015.

5.2 The Annual Information Governance Performance Report at Appendix 1 forms part of the Council's wider Information Governance Management and Reporting Framework, and is a key component of ensuring that the Council is undertaking adequate monitoring of its compliance with the above legislation.

5.3 The incoming General Data Protection Regulation will bring in significantly increased penalties for non-compliance with data protection law than currently apply. The maximum penalty for non-compliance with the General Data Protection Regulation is 4% of turnover, or €20 million, whichever is higher.

5.4 As outlined in this report, the General Data Protection Regulation introduces other changes to data protection law which the Council will be required to adhere to. The readiness approach outlined is focussed on ensuring that the Council will be in a position to comply with the provisions of the new General Data Protection Regulation when it comes into force, and mitigate the risk that the Council will be subject to enforcement action and financial penalty.

5.5 The UK Government has confirmed that the General Data Protection Regulation will be implemented into UK law, so it is not anticipated that the UK's exit from the EU will impact the Council's requirement to comply with GDPR.

## 6. MANAGEMENT OF RISK

6.1 Financial

The Annual Information Governance Report, as part of the Council's wider Information Assurance framework, forms part of the Council's mitigation against the risk of non-compliance with applicable Data Protection law, which may lead to enforcement action with monetary penalties and/or financial liability for damages to customers.

6.2 Employee

The Annual Information Governance Report, as part of the Council's wider Information Assurance framework, forms part of the Council's mitigation against the risk that our staff and elected members do not have the information they need to appropriately monitor and have oversight of the Council's information governance performance.

6.3 Customer

The Annual Information Governance Report, as part of the Council's wider Information Assurance framework, forms part of the Council's mitigation against the risk that customers are put at risk of harm due to inadequate management of personal data, and the risk that customers are unable to exercise their legal rights in relation to information and data held by the Council.

6.4 Environmental

No risks.

6.5 Technological

No risks.

6.6 Legal

The Annual Information Governance Report, as part of the Council's wider Information Assurance framework, forms part of the Council's mitigation against the risk that Council is exposed to enforcement or legal action resulting from non-compliance with information legislation.

6.7 Reputational

Realisation of any of the above risks would also be likely to lead to significant reputational damage to the Council.

## 7. IMPACT SECTION

7.1 Economy

Information and data are key assets of the Council, and recognised in the Aberdeen City Local Outcome Improvement Plan 2016-26 and the Strategic Aberdeen City Council Strategic Business Plan as critical enablers of the Council achieving its priorities for people, place and economy.

This Information Governance Report, as part of the Council's wider Information Governance Management & Reporting framework, forms part of the Council's assurance measures around our information, to ensure that it is fit to enable the Council to deliver outcomes for our people, place and economy.

7.2 People

As at section 7.1, above.

7.3 Place

As at section 7.1, above.

7.3 Technology

The General Data Protection Regulation requirements will need to be considered where technology is used by the Council to process personal data to ensure functionality meets our compliance requirements.

## 8. BACKGROUND PAPERS

Being Digital: A Transformation Strategy for the Council
Information Management Strategy

## 9. APPENDICES (if applicable)

**Appendix 1**: Annual Information Governance Report

## 10. REPORT AUTHOR DETAILS

Caroline Anderson
Information Manager
CAnderson@aberdeencity.gov.uk
01224 522521

Helen Cannings
Information Management Team
HCannings@aberdeencity.gov.uk
01224 523430

## HEAD OF SERVICE DETAILS

Simon Haston
Head of IT & Transformation
SHaston@aberdeencity.gov.uk
01224 523366