Agenda Item 7

# Audit and Standards Committee Report

| | |
|---|---|
| **Report of:** | **Executive Director of Resources** |
| **Date:** | **December 19th 2019** |
| **Subject:** | **Information Governance Annual Report** |
| **Author of Report:** | **Mark Gannon**<br>**Director of Business Change and Information Solutions** |

**Summary:**

The purpose of this report is to submit the Annual Information Governance Report for 2018/19 and to provide a brief update to the key information governance activities carried out since April 2019.

| | |
|---|---|
| **Recommendations:** | **Note progress and future annual report** |
| **Background Papers:** | Attached: Annual Information Governance Report 2018/19; Information Governance Framework; Information Asset Owners Brief |
| **Category of Report:** | OPEN |

## Statutory and Council Policy Checklist

| |
|---|
| **Financial Implications** |
| NO: |
| **Legal Implications** |
| YES |
| **Equality of Opportunity Implications** |
| NO |
| **Tackling Health Inequalities Implications** |
| NO |
| **Human rights Implications** |
| NO: |
| **Environmental and Sustainability implications** |
| NO |
| **Economic impact** |
| NO |
| **Community safety implications** |
| NO |
| **Human resources implications** |
| NO |
| **Property implications** |
| NO |
| **Area(s) affected** |
| None |
| **Relevant Cabinet Portfolio Member** |
| Councillor Terry Fox, Cabinet Member for Finance, Resources and Governance |
| **Is the item a matter which is reserved for approval by the City Council?** |
| NO |
| **Press release** |
| NO |

# REPORT TITLE: Information Governance

## 1.0 INTRODUCTION

1.1 The purpose of this report is to submit the Annual Information Governance Report for 2018/19 (Appendix A) and to provide a brief update to the key information governance activities carried out since April 2019.

## 2.0 BACKGROUND

2.1 In 2017, the Audit and Standards Committee asked the then Head of Information Management to provide an update to the Council's progress in the preparation for the General Data Protection Regulations (GDPR) that came into force on May 25th 2018.

2.2 The Information Management Team has subsequently provided updates to the Audit and Standards Committee and wants to formalise this with an Annual Information Governance Report to report on key information governance activity related to GDPR and other information rights, laws and regulations, and security requirements.

## 3.0 MAIN BODY OF THE REPORT

3.1 The focus of this Report is to submit the Annual Information Governance Report 2018/19, but to also provide the Committee with a brief overview to the key information governance activity and performance for this financial year (section 4).

3.2 The Information Governance Framework (Appendix B) and the Information Asset Owners Brief to Directors (Appendix C) have been included with this Report and are referred to at 4.11 and 4.12 respectively.

## 4.0 CURRENT UPDATE

4.1 This section provides an update to the key activities and performance between for this financial year (April 1st to December 2nd). The figures may be subject to slight change.

4.2 The Council has handled 230 data protection subject access requests. The performance target is 85% and the table below shows the performance is 81%. In comparison to last year, the number of requests has increased and performance has improved and stabilised. Of the 18 late requests, 14 requests were answered 7 days after the deadline.

| 2019/20 | Received | Answered in time | Answered Late | In Progress in time | In Progress, but late | Compliance % |
|---|---|---|---|---|---|---|
| **Qtr 1** | 93 | 88 | 5 | 0 | 0 | **95** |
| **Qtr 2** | 82 | 66 | 12 | 4 | 0 | **76** |
| **Qtr 3** | 55 | 33 | 1 | 21 | 0 | **60** |
| **Total** | **230** | **187** | **18** | **25** | **0** | **81** |

4.3 The Council has handled 1198 Freedom of Information Act and the Environmental Information Regulations requests. The performance target is 95% and the table below shows the target has been met, but is slightly lower than in previous years. This figure is being monitored to ensure it remains above the target level.

| 2019/20 | Valid | Answered in time | Answered late | Compliance % |
|---|---|---|---|---|
| **Qtr 1** | 468 | 449 | 19 | **95** |
| **Qtr 2** | 478 | 453 | 25 | **95** |
| **Qtr 3** | 252 | 238 | 14 | **95** |
| **Total** | **1198** | **1140** | **58** | **95** |

4.4 The Council has managed 138 information security incidents, of which 68 were personal data breaches. The table below shows a breakdown of the type of incidents:

| 2019/20 | Total reported | No. data breaches | ICO Notifications | Disclosure error | Lost or stolen | Online disclosure | Non-secure disposal | Cyber / Access Concerns |
|---|---|---|---|---|---|---|---|---|
| **Qtr 1** | 37 | 20 | 1 | 28 | 5 | 0 | 1 | 3 |
| **Qtr 2** | 58 | 33 | 1 | 42 | 8 | 1 | 0 | 7 |
| **Qtr 3** | 43 | 15 | 1 | 30 | 7 | 0 | 2 | 4 |
| **Total** | **138** | **68** | **3** | **100** | **20** | **1** | **3** | **14** |

4.5 The main type of incident being reported is Disclosure Error (100). The main cause is human error: emails sent to the wrong person (34), documents posted to the wrong address (32), and the remaining (34) a combination of documents lost, inaccurate data, documents left on printers, given to the wrong person.

4.6 The number of incidents reported is equivalent to 17 a month, which is less than the 20 a month of last year, but every incident carries a risk to the Council and the individuals affected because of the possible impact.

4.7 An organisation the size of Sheffield City Council and the number of processes, employees, partner agencies and systems and customers means it is not possible to eliminate incidents, so has to take appropriate measures to minimise the risks when handling information, especially personal data.

4.8 The Council's Internal Audit reviewed the Information Security Incident Procedure and gave it Limited Assurance. The Report recognised the good practice, but identified the improvement areas to improve:

a) Record keeping to ensure sufficient case records are held with a summarised report of the key facts, actions taken, manager sign off, and outcome;

b) Regular data analysis and reports to Directors and Senior Management to ensure they are aware of the incidents in their service area, to learn lessons, and take corrective action;

c) Review the current procedure and ensure officers are clear of their roles and responsibilities;

d) Review the Information Management essential learning and ensure it if fit for purpose, focused and accompanied by clear guidance so staff can apply best practice when handling information and reduce the risk of incidents;

e) Promote training and awareness. In March 2019, the Information Management Team confirmed to NHS Digital, in the Council's annual NHS Data Security and Protection Toolkit submission, that only 56% of staff had completed the essential Information Management learning training.

4.9 A follow up report has been submitted to the Executive Management Team to provide an update to the actions being taken about the Incident Procedure.

4.10 In addition to the above, work has continued to embed data protection practice across the Council with privacy notices, information sharing agreements, data protection impact assessments and data protection clauses and data processing agreements in contracts. Further work is still required, in particular to update existing contracts to ensure they are data protection compliant.

4.11 The Council's Information Governance Board has also updated the Information Governance Framework that clarifies key information governance policies, procedures, roles and responsibilities and staff training requirements. The Framework is attached for reference (Appendix B).

4.12 The Council's Information Governance Board also recommended that Directors would take the role of Information Asset Owners and a briefing note outlining the key responsibilities was taken to the Directors Group in October. The Information Asset Owners Brief to Directors is attached for reference (Appendix C).

4.13 Finally, the Council met the information and cyber security standards for the *National Cyber Security Centre's Cyber Essentials*, *NHS Data Security and Protection Toolkit* and *Payment Card Industry Data Security Standards*, and is working with the Cabinet Office to submit to the Public Services Network Code of Connection.

## 5.0 RECOMMENDATIONS

5.1 The Committee to note the Annual Information Governance Report 2018/19 and to confirm if it wishes for a similar report in future.

This page is intentionally left blank