Audit & Governance Committee **7 December 2016**

Report of the Director of Customer and Corporate Services

Information Governance & Freedom of Information Report (including information security)

1. This report provides Members with updates or reports for :

- information governance performance
- the new General Data Protection Regulation (GDPR)
- the Information Commissioners Office (ICO) data protection audit and recommendations
- compliance with the Local Government Transparency Code 2015 (LGTC 2015)
- the Health and Social Care Information Centre (HSCIC) Information Governance Toolkit (IG Toolkit) update
- information security checks

2. Information Governance Performance

2.1 Information governance activities were brought in house (from April 2015 onwards) having previously been provided by Veritau. The staggered transfer was fully completed early this year.

2.2 During the course of the handover the Council accepted an offer from the ICO to audit the Council's information governance processes. The focus of that audit was data protection. FOI performance was not audited as the Council had made considerable improvements in its FOI and EIR performance. Using the same methodology for in-time compliance as previous, we achieved in-time compliance for April 2015 to March 2016 of 95.6%. In 2014/15 this was 93.9% and in 2013/14, it was 81%. See annex 1 for 2015/16 report

2.3 We have also made significant performance improvements for in-time compliance with Data Protection Act Subject Access to Records requests (SARs). This was a specific area that ICO auditors recommended we improve upon. Again, using the same methodology for in-time compliance as previous years, we achieved in-time

compliance for April 2015 to March 2016 of 77.1%. See annex 1 for 2015/16 report

2.4 From 1st April 2016 to 31st October 2016, there has been 6 decision notices by the Information Commissioner's Office (ICO) for the council.

- 4 upheld the council's responses and actions
- 1 partly upheld the council's response and action
- 1 did not uphold the council's action as we had not responded in time

Decision notices are published on the ICO's website – see below

https://search.ico.org.uk/ico/search?q=decision+notices

However there is one decision notice that has been removed currently by the ICO. This is regarding an upheld decision on the application of FOI act exemption under section 14 (vexatiousness).

3. The new General Data Protection Regulation (GDPR)

3.1 The GDPR will take effect from May 2018, and will introduce significant changes to the current data protection rules in the Data Protection Act 1998.

3.2 With the approval of the GDPR, we will need to adapt our approaches, procedures, and security policies. It will be crucial for services, particularly those responsible for a database or system to understand these emerging GDPR requirements in addition to how staff, processes, policies, and technologies may need to be changed in order to accommodate them. We will need to establish strong controls around personal information and to take full accountability for the controls in place.

3.3 Substantial guidance is expected to be produced over the next 6 to 12 months both by the ICO and at a European level.

3.4 We are working to ensure arrangements are in place to prepare for and meet the requirements of the GDPR across all services. Failure to prepare leading to compliance failures could have serious consequences for the council corporately, including substantial fines. It is therefore it is essential that there is a corporate mechanism to coordinate arrangements. It may be helpful at this time, to note that many of the ICO audit recommendations and actions, as well as the

areas the ICO auditors picked up as areas of good practice, had the GDPR in mind.

4. ICO data protection audit report and recommendations

4.1 The ICO's audit findings identified areas for improvement in our existing arrangements for data protection compliance and issued us with a set of recommendations. The Council developed an action plan in response to these recommendations. The delivery of this action plan was followed up by the ICO who concluded that no further follow up was required. All but one action had commenced but there were a number of incomplete actions. Significantly there was outstanding work to be done relating to records management, staff training and data sharing.

4.2 This work is still ongoing but there has been further progress including:

- The design of several information governance training packages with the first – Data Protection Act Essentials – being delivered to all staff via the intranet.

- The design, build and testing of an online tool/app for our "information asset register" (IAR) which will be launched soon.

- Implementation of further organisational and technical measures to improve our information security.

4.3 The IAR is a key tool for improving our management of information. It will help manage risks such as where personal information may be being shared without appropriate agreements in place or where data is at risk of being kept for longer than it should be.

4.4 The table which follows shows the current state of play with regards to the implementation of the action plan. The fact that there are still actions which are only partially completed reflects the fact that the legislative framework, data standards and guidance are changing and the steps required to complete the actions will need to be consistent with these changes.

Scope area	Number of recommendations in each scope area from the original audit report	Number of actions complete, partially complete and not implemented – as reported to Committee in June 2016	Number of actions complete, partially complete and not implemented – as reported to Committee in June 2016
Records Management	41	13 Complete 27 Partially complete 1 Not implemented	29 Complete 12Partially complete 0 Not implemented
Subject Access Requests	25	6 Complete 19 Partially complete 0 Not implemented	20 Complete 5 Partially complete 0Not implemented
Data Sharing	24	12 Complete 12 Partially complete 0 Not implemented	22Complete 2Partially complete 0 Not implemented

5. Compliance report and update on the Local Government Transparency Code 2015 (LGTC 2015)

5.1 The council meets its requirements by publishing information on either the relevant website pages or through the York Open Data platform. The link to the LGTC 2015 information on the YOD platform is

https://www.yorkopendata.org/

5.2 Compliance with the LGTC 2015 is monitored and reported throughout the year via the Governance, Risk and Assurance Group (GRAG) and further to the report to Committee in June; a compliance report is at annex 2 for your information.

5.3 The Government recently undertook consultation on the proposals to update the LGTC 2015. Any changes will require secondary legislation to revoke the existing code and put a new updated code in place.

6. Health and Social Care Information Centre (HSCIC)

6.1 The council has to undergo assessment to attain the appropriate level of assurance to be able to use certain Health service systems. The IG Toolkit is a Department of Health (DH) Policy delivery vehicle that HSCIC is commissioned to develop and maintain. It draws together the legal rules and central guidance set out by DH policy and presents them in a single standard as a set of information governance requirements.

6.2 We retained the required level of assurance including an improvement this year (Version 13) against last year (Version 12). Further details are at Annex 3.

6.3 The next assessment has to be completed by 31st March 2017. This will present new challenges particularly as certain evidence requirements have changed. An action plan will be completed and monitored through the GRAG.

6.4 New data security standard for health and social care have recently been the subject of consultation. We are working closely with ICT and the relevant service areas to ensure we can apply the final approved security standards, consent and opt-outs, as they will apply to every organisation handling health and social care information.

7. Information Security Checks

7.1 In accordance with the agreed audit plan, information security checks are being undertaken during 2016/17. The purpose of these checks is to assess the extent to which confidential, personal or sensitive data is stored securely and to ensure that data security is being given sufficient priority within the council.

8. Consultation

Not relevant for the purpose of this report.

9. Options

Not relevant for the purpose of this report.

10. Analysis

Not relevant for the purpose of this report.

11. Council Plan

11.1 The council's information governance framework offers assurance to its customers, employees, contractors, partners and other stakeholders that all information, including confidential and personal information, is dealt with in accordance with legislation and regulations and its confidentiality, integrity and availability is appropriately protected.

12. Implications

12.1 Relevant implications are set out in the body of the report

13. Risk Management

13.1 The council may face financial and reputational risks if the information it holds is not managed and protected effectively. For example, the ICO can impose civil monetary penalties up to £500k for serious data security breaches (this may be increased following the signing of the General Data Protection Regulation (GDPR). The failure to identify and manage information risks may diminish the council's overall effectiveness. Individual(s) may be at risk of committing criminal offences. For example, under section 55 and/or section 61 of the Data Protection Act (DPA) 1998

14. Recommendations

Members are asked:

- To note the sustained performance levels
- To give a commitment to support the work required to implement the General Data Protection regulation
- To note the ongoing work required to ensure the Council meets its information governance responsibilities.

Reason: To ensure that Members are kept updated on information governance issues.

Contact Details

Author:

Lorraine Lunt
Information Governance & Feedback Team Manager
Telephone: 01904 552247

Chief Officer Responsible for the report:

Andy Docherty

Assistant Director

Telephone: 01904 551004

Report Approved	√	**Date**	28th November 2016

Wards Affected: List wards or tick box to indicate all **All** √

For further information please contact the author of the report

Annexes

Annex 1 – 2015/2016 performance report
Annex 2 – Transparency Code Indicators report
Annex 3 – HSCIC IG toolkit

Background Information

Not applicable

Glossary

DH	Department of Health
DPA	Data Protection Act
EIR	Environmental Information Regulations
FOI	Freedom of Information
GDPR	General Data Protection Regulation
GRAG	Governance, Risk and Assurance Group
HSCIC	Health and Social Care Information Centre
IAR	Information Asset Register
IG	Information Governance
LGTC	Local Government Transparency Code
ICO	Information Commissioners Office
SARS	Subject Access to Records
YOD	York Open Data