Public Session

Report Reference Number: A/17/19 **Agenda Item No: 7**

To:	**Audit and Governance Committee**
Date:	**17 January 2018**
Author:	**Gillian Marshall, Solicitor to the Council**
Lead Officer:	**Karen Iveson, Executive Director (s151)**

Title: Information Governance Annual Report

Summary:

In March 2014 the Council's internal auditors (Veritau) published a final report into their review of the Information Governance and Data Protection arrangements at Selby District Council.

A project was established with a view to putting in place systems and controls to address the issues identified during the audit. As part of that Information Governance was added to the Terms of Reference for Audit and Governance Committee and it was agreed that an annual report on the Information Governance arrangements would be provided for the Committee. An action plan was approved to address the identified issues.

This is the annual report for 2017.

Recommendations:

i. **That Audit and Governance Committee note the contents of this report.**

Reasons for recommendation

To meet the requirement within the Audit and Governance Committee Terms of Reference and the 2014 audit action plan.

1. Introduction and background

1.1 In March 2014 the Council's internal auditors (Veritau) published a final report into their review of the Information Governance and Data Protection arrangements at Selby District Council. It was found that the arrangements for managing risk were poor with significant control weaknesses in key areas and major improvements required before an effective control environment would be in operation. Their overall opinion of the controls within the system at the time of the audit was that they provided **Limited Assurance**. A project was established with a view to putting in place systems and controls to address the issues identified during the audit and an Action Plan was put in place. This plan was updated as the original actions were completed and following the further Audits outlined below new matters were identified and added to the plan.

1.2 In accordance with the Action Plan the Executive Director (s151) (now Chief Finance Officer) was appointed to the post of Senior Information Risk Officer (SIRO) with overall responsibility for information governance (IG). Day to day oversight of the IG arrangements is the responsibility of the Solicitor to the Council.

1.3 An Information Governance Framework consisting of an Information Charter, Information Risk Management Policy, ICT Acceptable Usage Policy, Data Protection Breach Policy and a Document Retention Policy was approved in 2014. However, these policies are in the process of being reviewed to reflect changes required by the General Data Protection Regulation (GDPR) which comes into force in May 2018.

1.4 All staff received briefings in 2014 on the new IG Framework and further mandatory training was rolled out. IG is now included in induction briefings. Further staff training is proposed as part of the preparations for GDPR.

1.5 In 2015 and 2017 Veritau published final reports in relation to Information Security checks. The key finding of the reports is that the Council is reasonably well protected against accidental disclosure of information. Some improvements were recommended to ensure the clear desk policy was reinforced, that lockable cupboards were available and that the archive rooms be secured. These were added to the Action Plan. Regular messages are now provided to staff regarding information security and lockable cupboards are provided.

1.6 In October 2016 Veritau reported in relation to Information Governance and Freedom of Information and gave an opinion of reasonable assurance. The key finding of the report in relation to Information Governance is that the Council had made significant progress since the audit of information governance in 2013-14, but that there remained some weaknesses. The resultant actions were added to the Action Plan attached at Appendix A. In relation to information requests the key finding was that the Council has a well defined system in place to administer and respond to information requests, however at that time the Council was not meeting the 86% target for

responding within 20 working days. Resultant actions to address matters were added to the Action Plan.

2 The Report

2.1 This report provides an update on information governance issues matters during 2017.

2.2 Information sharing agreements

The council remains a signatory to the North Yorkshire Multi Agency Information Sharing Protocol.

The Council completed a variation to a data sharing agreement in relation to the settlement of Syrian refugees in the District.

2.3 Information Security checks

Veritau carried out information security checks at the Civic Centre in March 2017. The purpose of the checks were to test the systems in place and 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 council offices.

Overall, the checks established that the Council is reasonably well protected against accidental disclosure of information. However, weaknesses were identified some of which have largely been addressed following the organisational review and the remaining items still on the Action Plan will be addressed this year.

2.4 Data Protection Breaches

Within the Council a number of data security incidents have been investigated since the last report to Committee in January 2017. The incidents included a lost Blackberry, a stolen laptop, the mis-identification of a customer causing details of the wrong debt to be discussed, sensitive e mail and letters sent to incorrect addresses

The incidents were subject to formal breach reviews by the relevant Service Managers. None were at a level that required reporting to the Information Commissioner. Apologies were given to affected customers.

Recommendations arising from the breach investigations were implemented locally.

This represents an increase in incidents from the previous year but this is considered to be the result of increased awareness of both the requirements around data breaches and the correct procedure. The purpose of the

procedure is to document breaches so that lessons can be learned and procedures can be updated.

2.5 Freedom of Information

The Key Finding of the report in 2016/7 was that the Council currently has a well defined system in place to administer and respond to FOI requests, however, it was currently not meeting the 86% target for responding within 20 working days. Following the re-introduction of a system for chasing responses from service areas before they are due and also introducing an escalation process to senior management if a response is at imminent risk of being classified late, the Council's response rate for 2017 has increased to 95.45% completed in time

The table below shows the number of FOI requests received and responded to in 2017 which shows a response "in time" of 95.45%.

Month	Received	Outstanding	Completed	% in time	% out of time
Jan-17	63	0	63	100.00%	0.00%
Feb-17	55	0	55	100.00%	0.00%
Mar-17	52	0	50	96.15%	0.00%
Apr-17	42	0	42	100.00%	0.00%
May-17	44	0	44	100.00%	0.00%
Jun-17	60	1	58	96.67%	1.67%
Jul-17	42	0	42	100.00%	0.00%
Aug-17	60	0	60	100.00%	0.00%
Sep-17	39	0	39	100.00%	0.00%
Oct-17	46	0	46	100.00%	0.00%
Nov-17	60	3	57	95.00%	5.00%
Dec-17	33	14	19	57.58%	42.42%
TOTAL	**596**	**18**	**575**	**95.45%**	**4.09%**

The Council's performance data for 2015 reported to the Audit Committee showed a response "in time" rate of 77.59%. The performance data reported for 2016 showed a response "in time" rate of 80.18%.

The target being worked to remains 86% as the Information Commissioner will consider formal performance monitoring of an authority where it responds to 85% or fewer requests within the statutory time period. Performance during 2017 has been well above target. Legal Services and Business Support continue to work with service areas to ensure that requests are responded to within statutory time limits.

2.6 Information Governance Action Plan

The Action Plan at Appendix A indicates a small number of Actions which require completion. With the exception of physical security measures which are to be completed by March 2018, most of these will be part of the implementation plan for GDPR which must be completed by May 2018.

3 Legal/Financial Controls and other Policy matters

Legal Issues

3.1 The Information Commissioner has the power to fine the Council if there is a serious breach and he concludes that the Council does not have procedures in place that are sufficiently robust

Financial Issues

3.2 In relation to the resource required for implementing GDPR consideration is being given as to how the resource is to be obtained and at what financial costs.

Impact Assessment

3.3 Residents, suppliers, customers and partners have a reasonable expectation that the Council will hold and safeguard their data appropriately. Failure to comply with recognised good practice will have a negative impact of the reputation of the organisation.

4. Conclusion

4.1 The overall levels of control are within reasonable levels and the existing framework operates satisfactorily. Remaining Actions from the Action Plan will be subsumed into the GDPR Implementation Plan.

5. Background Documents

None

Contact Officer:

Gillian Marshall
Solicitor to the Council
Selby District Council
gmarshall@Selby.gov.uk

Appendices:

Appendix A - High Level Action Plan as at 03.01.2018