SELBY DISTRICT COUNCIL

Report Reference Number: A/18/13

To:	**Audit and Governance Committee**
Date:	**30 January 2019**
Author:	**Caroline Fleming, Senior Solicitor**
Lead Officer:	**Stuart Robinson, Head of Business Development & Improvement**

Title: Information Governance Annual Report

Summary:

This is the Council's annual report on Information Governance arrangements for 2018.

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.

1. Introduction and background

1.1 The current arrangement of annual reporting started following the Council's internal auditors (Veritau) publishing their report into their review of the Information Governance and Data Protection arrangements at Selby District Council In 2014. A project was established with a view to putting in place systems and controls to address the issues identified and the plan was updated as the original actions were completed. Subsequent audits took place and 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.

1.2 To reflect changes brought about by the General Data Protection Regulation (GDPR) a new Information Governance Strategy and polices have been put in place. A Central Information Governance Group (CIGG) was set up with terms of reference and membership from Legal, Policy and Performance, Business Development and Improvement, Data and Systems, Customers, Development Management, Contracts and Commissioning, Democratic Services. Operations and Veritau to monitor compliance.

1.3 All staff received briefings on the GDPR on 16 April, 25 April and 4 May 2018 and further mandatory training was rolled out. IG is included in induction briefings.

1.4 In 2018 Veritau published a report in relation to the Information Security check for 2018. As for the report for 2016/2017 the key finding of the report is that the Council is reasonably well protected against accidental disclosure of information.

2. The Report

2.1 This report sets out the information governance issues that have arisen during 2018.

2.2 <u>General Data Protection Regulation (GDPR)</u>

The GDPR came into force on 25th May 2018 and the Data Protection Act 1998 has been replaced by the Data Protection Act 2018. It is expected that the provisions of the GDPR will remain in force post-Brexit, and for the foreseeable future.

Although in general the principles of data protection remain similar, there is greater focus on evidence-based compliance with specified requirements for transparency, more extensive rights for data subjects and considerably harsher penalties for non-compliance. The GDPR introduces a principle of *'accountability'*. This requires that organisations must be able to *demonstrate compliance*.

The new data protection legislation requires that the Council has a Data Protection Officer. Veritau Limited undertake this role on behalf of Selby District Council. In addition an information asset register has been produced to understand the Council's information assets and the risks to them.

Veritau and the CIGG have identified priority areas going forward in relation to the Information Asset Registers, Privacy Notices, training, policy review, communications and the preparation of an information governance strategy for 2019-20.

2.3 <u>Information sharing agreements</u>

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

The Council is in the process of completing a variation to data sharing agreements in relation to the settlement of Syrian refugees in the District to reflect changes brought about by GDPR.

The CIGG action plan includes an action to review information sharing arrangements in 2019.

2.4 Information Security checks

Veritau carried out an information security check at the Civic Centre in 2018. The purpose of the check was 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.

The last check was in 2018. Overall, the checks established that the Council is reasonably well protected against accidental disclosure of information. However, weaknesses were identified such as lack of key safes and unclear desks which have since been addressed.

2.5 Data Protection Breaches

The number of data protection breaches 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 beaches so that lessons can be learned and procedures can be updated. Data breaches are monitored through the CIGG.

Within the Council a number of data security incidents have been investigated since the last report to Committee in January 2017.

The first breach in January 2018 was at a level that required reporting to the ICO who decided that the data protection breach did not meet their criteria for formal enforcement action. The Council took action in relation to recommendations that arose following its own investigation which included further data protection and software training and quality management of information held. The remaining breaches were identified as amber and did not reach the threshold of referral to the ICO. The incidents were:

Disclosure of personal details on planning portal
Email sent to address in corporate address book in error
Benefit notification letter sent to wrong person
Annual bill sent to wrong person
Rent arrears collection letter sent to wrong person
Council tax bill & Housing benefit entitlement letter sent to wrong person
Council tax bill sent to wrong person
Acknowledgement letter sent to wrong person
Award letter sent to wrong person
Email sent to wrong person
disclosure of personal details on planning portal
Letter sent to wrong person

Personal email addresses sent to others
Invoice request sent to wrong email address
Email forwarded to local authority in error
Email forwarded with another customers email
Signature on public access
Witness statement sent to wrong person
Email sent with another person's work mobile number

Each incident was subject to a formal breach review by the relevant Lead Officer. Recommendations arising from the breach investigations were implemented locally.

2.6 Freedom of Information

The key findings of the report are that the Council currently has a well defined system in place to administer and respond to FOI requests. As reported in January 2017 the Council's response rate was 80.18% completed in time. 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 "in time" response rate increased.

The table below shows the number of FOI requests received and responded to in 2018 which shows a response "in time" of 90.42%.

Month	Received	Outstanding	Completed	% in time (20 days)	% out of time (20 days)
Jan-18	61	0	61	90.16%	9.84%
Feb-18	68	0	67	88.06%	11.94%
Mar-18	59	0	59	84.75%	15.25%
Apr-18	69	0	69	94.20%	5.80%
May-18	54	0	54	88.89%	11.11%
Jun-18	60	0	60	93.33%	6.67%
Jul-18	68	0	68	88.24%	11.76%
Aug-18	67	0	67	88.06%	11.94%
Sep-18	45	0	44	88.64%	11.36%
Oct-18	63	1	62	88.71%	11.29%
Nov-18	52	2	50	92.00%	8.00%
Dec-18	38	5	33	100.00%	0.00%
Total	**704**	**8**	**694**	**90.42%**	**9.58%**

The Council's performance data for 2015 reported to the Audit and Governance Committee showed a response "in time" rate of 77.59%. The performance data reported for 2016 and 2017 showed a response "in time" rate of 80.18% and 95.45% respectively.

The target being worked to is 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 2018 has been above target. Legal Services and Business Support continue to work with service areas to ensure that requests are responded to within statutory time limits.

The CIGG will be reviewing the requests and look at “repeat requests” and publication on the website.

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 There are no financial issues in this report.

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.

5. Background Documents

None

Contact Officer:

Caroline Fleming
Senior Solicitor
Selby District Council
cfleming@selby.gov.uk