APPENDIX 3

SELBY
DISTRICT COUNCIL

Selby District Council

Information Governance Progress Report 2018/19

Veritau
Assurance Services for the Public Sector

Information Governance Manager:	Rebecca Bradley
Head of Internal Audit:	Max Thomas
Date:	10th April 2019

PURPOSE OF THE REPORT

1 To provide an update on Information Governance matters and developments in the Council's Information Governance arrangements and compliance with relevant legislation.

BACKGROUND

2 Information governance is the framework established for managing, recording, protecting, using and sharing information assets in order to support the efficient and effective delivery of services. The framework includes management structures, policies and processes, technical measures and action plans. It helps to ensure information is handled securely and correctly, and provides assurance to the public, partners and other stakeholders that the Council is complying with all statutory, regulatory and best practice requirements. Information is a key asset for the Council along with money, property and human resources, and must therefore be protected accordingly. Information governance is however the responsibility of all employees.

3 The Council must comply with relevant legislation, including:

- The Data Protection Act 2018
- The General Data Protection Regulation (GDPR)
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Regulation of Investigatory Powers Act 2000

4 In March 2018, the Council appointed Veritau to be its statutory Data Protection Officer (DPO).

5 The General Data Protection Regulation (GDPR) and the newly updated Data Protection Act came into force in May 2018. A working group comprising officers and representatives from Veritau was established and an intensive programme of work was undertaken to prepare for the new legislation.

6 The Corporate Information Governance Group (CIGG) is responsible for overseeing information governance within the council. The group is chaired by the Head of Business Development and Improvement and provides overall direction and guidance on all information governance matters. CIGG also helps to support the Council's Senior Information Risk Owner (SIRO) to discharge her responsibilities. CIGG is currently coordinating the delivery of the GDPR action plan, which includes reviewing and updating the council's information governance strategy and policy framework. CIGG has met regularly during the year.

7 All public authorities are required to appoint a Data Protection Officer (DPO). The DPO is responsible for monitoring and reporting on compliance with data protection legislation. The DPO also provides independent advice on data protection matters. The DPO also advises on Data Protection Impact Assessments and acts as the first point of contact for the Information Commissioner's Office (ICO) and data subjects.

GDPR ACTION PLAN UPDATE

8 The corporate privacy notice has been updated and is available on the Council's website. Individual privacy notices are also being prepared by each service team. These are being reviewed by Veritau as they are completed and will be published on the website.

9 Work is also ongoing to review and update the information governance policy framework.

10 The Information Asset Register has been amended to reflect GDPR compliance needs. Work is ongoing to ensure the register is correct and up to date. Veritau is working with the relevant service teams to complete this work. A summary of this progress has been included in the Internal Audit Progress Report (Appendix 1, Annex 3). This work is expected to be completed by 30 June 2019.

TRAINING

11 The Council and Veritau successfully delivered a series of GDPR briefing sessions to all Council officers in March, April, and May 2018. However, it is recognised that some teams will require further service specific training sessions. These service specific training sessions are now being planned.

12 Veritau is also planning to deliver a series of other training sessions including Data Protection Principles and Rights; Introduction to Records Management; and Elected Members Data Protection Induction Briefing.

INFORMATION SECURITY INCIDENTS (DATA BREACHES)

13 Information Security Incidents have been reported to Veritau as required. The incidents are assessed, given a RAG rating and then investigated as required. Green incidents are unlikely to result in harm but indicate a breach of procedure or policy; Amber incidents represent actual disclosure, but harm is unlikely to be serious; and Red incidents are sufficiently serious to be considered for self-reporting to the ICO. Some incidents are categorised as 'white'. White incidents are where there has been a failure of security safeguards but no breach of confidentiality, integrity, or availability has actually taken place (i.e. the incident was a near miss). None of the reported incidents have needed to be reported to the Information Commissioner's Office (ICO).

14 The number of Security Incidents reported to Veritau in 2018-19 are as follows:

Year	Quarter	Red	Amber	Green	White	Total
2018/19	Q1	0	0	0	0	0
	Q2	0	0	0	0	0
	Q3	0	1	1	1	3
	Q4	1	2	0	0	3
	Total	1	3	1	1	6