NORTH YORKSHIRE COUNTY COUNCIL

AUDIT COMMITTEE

22 MARCH 2021

INFORMATION GOVERNANCE ANNUAL REPORT

Report of the Corporate Director – Strategic Resources

1.0 PURPOSE OF THE REPORT

1.1 To provide an update on Information Governance matters, developments in the County Council's Information Governance arrangements, details of related performance and compliance with relevant legislation.

2.0 BACKGROUND

2.1 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 County Council is complying with all statutory, regulatory and best practice requirements. Information is a key asset for the County Council along with money, property and human resources, and must therefore be protected accordingly. Information governance is however the responsibility of all employees.

2.2 The County Council must comply with relevant legislation, including:

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

2.3 In respect of Information Governance, the Audit Committee is responsible for:

- Reviewing all corporate policies and procedures in relation to Information Governance
- Overseeing the implementation of Information Governance policies and procedures throughout the County Council

2.4 Information governance has been identified as a high risk area on the corporate risk register. This is in part due to the consequences should the County Council suffer a serious data breach. As well as regulatory action, including the possibility of financial penalties, the County Council could also suffer significant reputational damage in such an event.

3.0 ROLES AND RESPONSIBILITIES

3.1 The County Council's information governance framework includes a number of specific roles, as follows:

Senior Information Risk Owner (SIRO)

The Corporate Director - Strategic Resources has been designated as the Senior Information Risk Owner (SIRO) with specific responsibility for ensuring risks relating to information governance are managed effectively. The SIRO reports on the County Council's management of information risks to Management Board and the Audit Committee.

Corporate Information Governance Group (CIGG)

The Corporate Information Governance Group (CIGG) exists to support the SIRO in the discharge of those responsibilities. CIGG provides overall direction and guidance on all information governance matters. CIGG meets every two months and reviews and updates the information governance strategy and policy framework, monitors information risks and emerging issues, develops and coordinates action plans and oversees related activities.

Data Protection Officer (DPO) – Veritau

All public authorities are required to appoint a Data Protection Officer (DPO). The DPO monitors and reports on compliance, and 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. Veritau is the County Council's Data Protection Officer

Data Governance Team

The Data Governance team works with service areas to embed information governance policies and best practice. This includes providing support with the preparation and maintenance of information asset registers, Data Protection Impact Assessments and information sharing agreements. The team supports services to mitigate the risk of data breaches. The team also delivers classroom based training to service teams and updates the mandatory data protection e-learning courses.

Veritau Information Governance Team

The Information Governance team within Veritau manage all Freedom of Information and Subject Access requests received by the County Council. The team coordinates responses, provides advice to services on the use of exemptions and responds to complaints. The team chairs the Multi Agency Information Sharing Protocol group and investigates all serious data breaches. The team also works with the Data Governance team to ensure the policy framework is kept up to date, raise awareness of data protection obligations, and respond to any emerging issues.

4.0 POLICY FRAMEWORK / COMPLIANCE WITH UK-GDPR / DPA 2018

4.1 The information governance policy framework was updated in preparation for the implementation of GDPR / DPA 2018 in May 2018. Individual policies are continuing to be reviewed and updated as necessary to reflect best practice and guidance issued by the ICO. The policies and other documentation are now also being updated as a result of the UK leaving the EU to ensure reference is made to UK-GDPR.

4.2 An Information Governance and Management Strategy has been approved by CIGG. The Strategy builds on the work done to prepare for GDPR (now UK-GDPR) and DPA 2018, and helps the County Council to address new and emerging information risks. The priorities include raising awareness of information governance, embedding procedures across the County Council to better understand and manage information assets and risks, continued compliance with all relevant legal requirements, and the utilisation of new technologies and innovations to improve service delivery. The Strategy also aims to develop policies and processes to support improved information and records management across the County Council.

4.2 Key actions completed in the year and other developments have included:

- Receiving the results of a Data Protection compliance audit completed by Veritau and agreeing a detailed action plan to address the findings from the review.
- Launching a new template and guidance document for completing Data Protection Impact Assessments.
- Approving a new information security incident categorisation process and a Policy for Processing Special Categories of Data
- Information Asset Registers have been prepared by each directorate, and these are subject to ongoing review. The registers identify all information assets and their associated information asset owners.
- Privacy notices have been prepared and published on the Council's website for most services. These are continuing to be reviewed with updates actioned where required.
- Supplies and services are continuing to be reviewed to identify any remaining contracts or processing activity involving personal information. Any new agreements will be checked to ensure that they now reference the UK-GDPR.
- Areas who carry out Law Enforcement processing which is covered by Part 3 of Data Protection Act 2018 have been identified. Work is ongoing to update documentation including privacy notices.

5.0 DATA BREACHES

5.1 Employees are required to report all information security incidents (data breaches) to Veritau, including any near misses. The incidents are assessed, given a RAG rating and then investigated.

5.2 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. 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).

5.3 The number of reported data security incidents since April 2019 is as follows:

Year	Quarter	Red	Amber	Green	White	Total
2019/20	Q1	5	45	17	14	81
	Q2	4	24	28	21	77
	Q3	11	33	21	19	84
	Q4	17	46	28	16	107
2020/21	Q1	0	29	14	12	55
	Q2	2	24	27	21	74
	Q3	4	21	39	9	73
	Q4	2	6	30	7	45

5.4 Two data breaches have been reported to the ICO in 2020/21 to date, as follows:

Type of breach	ICO Action
Lost/misplaced data	No further action
Unauthorised disclosure/access to data	ICO responded with recommendations

6.0 CYBER SECURITY

6.1 The impact of a significant cyber attack against the council as well as making systems unavailable can create a significant data breach. During the last year two authorities have been impacted by an attack which caused the loss of service to residents and potential data loss. It has been published that the cost of recovery for one of these councils has been in excess of £10 million.

6.2 To mitigate this the Technology and Change service have invested in and continue to maintain several technical measures to minimise the likelihood of an attack and reduce the impact if one occurs.

6.3 As these measures cannot guarantee that the council will not be effected by a cyber incident, our employees have an important role to play as the last line of defence

and the Technology and Change Service provide regular advice and guidance to them through training and regular Intranet updates and key messages.

6.4 A revised set of training will be released during the next 6 months to update employees on how to work securely and regular simulations will be carried out to improve the ability to identify a phishing email and what actions they should take if they have one.

6.4 The Technology & Change Service has continued to maintain its ISO 27001 certification, which is an internationally recognised framework for Information Security ensuring that the Confidentiality, Integrity and Availability of data is maintained. The Service has also achieved ISO/IEC 20000 certification which relates to best practice for IT service management (ITSM). This helps organisations to evaluate how effectively they deliver managed services, measure service levels and assess their performance.

7.0 COVID-19 PANDEMIC

7.1 A significant amount of work was undertaken in response to the Covid-19 pandemic, particularly in the early part of the year. This included preparing an overarching data privacy notice and specific privacy notices for some processing activity. Information sharing agreements were arranged with key partners and Data Protection Impact Assessments completed where new processes were introduced and other operational changes made. In addition, guidance from the ICO and the Government on data protection risks and implications was disseminated across the Council and to stakeholders. This included guidance on document retention and safe data protection practices for staff working at home.

8.0 OFFICE 365 IMPLEMENTATION

8.1 As part of the Office 365 implementation the ability to classify documents (email, word, excel) under the agreed protective marking scheme (Official, Official Sensitive) has been improved to make it easier for the end user and where possible automate the classification based on the content of the document.

8.2 Within Office 365 the ability to categorise documents allows us to put in place retention policies which supports one of the General Data Protection Regulations requirements of storing data no longer than is necessary for the purposes for which it was processed. Work is ongoing in this area with the Data Governance team working with service areas to identify retention periods.

8.3 Other functionality within Office 365 will be rolled out during the year to further improve our ability to manage information securely and effectively.

9.0 RECOMMENDATION

9.1 Members are asked to note the progress made in developing the County Council's information governance arrangements during the year.

Report prepared by Max Thomas, Head of Internal Audit and Jon Learoyd, Head of Technology Solutions

GARY FIELDING
Corporate Director – Strategic Resources

County Hall
Northallerton

4 March 2021

Background Documents: Relevant reports considered by the Corporate Information Governance Group