NORTH YORKSHIRE COUNTY COUNCIL

AUDIT COMMITTEE

21 MARCH 2022

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 continues to be reviewed and updated to comply with UK-GDPR and the DPA 2018, and to reflect the latest best practice guidance issued by the ICO.

4.2 The Information Governance and Management Strategy has been updated. The current priorities include continuing to raise awareness of information governance responsibilities and good practice across the County Council, embedding procedures to better understand and manage information assets and risks, and the utilisation of new technologies and innovations to improve security and service delivery. The Strategy also aims to develop policies and processes to support improved information and records management across the County Council.

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

- the implementation of a new information security incident categorisation process
- the identification and review of service areas carrying out law enforcement processing covered by Part 3 of the Data Protection Act 2018. Work is ongoing to update relevant documentation including privacy notices with the initial focus being on Trading Standards
- providing specialist workshops on Data Protection Impact Assessments utilising the new template and guidance as well as law enforcement processing
- producing guidance for information asset owners
- completing a data protection compliance review in Technology and Change
- reviewing and updating privacy notices as required
- reviewing supplies and services to identify any remaining contracts or processing activity involving personal information. Any new agreements will be checked to ensure that they reference the UK-GDPR.

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 risk rating and then investigated.

5.2 Low or very low risk incidents are unlikely to result in harm but indicate a breach of procedure or policy; moderate incidents represent actual disclosure, but harm is unlikely to be serious; and high or very high incidents are sufficiently serious to require self-reporting to the ICO and potentially the data subjects. 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 in the period 1 April 2020 to 31 December 2021 is as follows:

2021 / 22							
Quarter	**Very high**	**High**	**Moderate**	**Low**	**Very low**	**White**	**Total**
Q1	4	0	10	29	23	14	80
Q2	2	1	13	27	29	18	90
Q3	2	0	16	36	17	30	101

5.4 The risk assessment methodology has been changed but the equivalent number of data security incidents reported in 2020/21 was as follows:

2020 / 21					
Quarter	**Red**	**Amber**	**Green**	**White**	**Total**
Q1	0	29	14	12	55
Q2	2	24	27	21	74
Q3	4	21	39	9	73
Q4	2	6	30	7	45

5.5 9 data breaches have been reported to the ICO in 2021/22 to date, as follows:

Type of breach	ICO Action
s170 unauthorised access	No further action
s170 unauthorised access	No further action
Incorrect document recipients	No further action
Unauthorised disclosure	No further action
s170 unauthorised access	No further action
Loss of records	No further action
s170 unauthorised access	No further action
s170 unauthorised access	No further action
Incorrect document recipients	ICO still investigating

6.0 LOCAL GOVERNMENT REORGANISATION (LGR)

6.1 Work is ongoing to ensure the new council will be compliant with the Data Protection Act 2018 / UK-GDPR from 1 April 2023. This work includes reviewing the existing policies and processes for each of the North Yorkshire councils, and adopting a standard framework. Support is also being provided to the LGR programme to ensure data protection risks are identified and managed as services and systems are brought together. Data protection impact assessments are therefore being completed for each work stream and individual transformation project as required.

6.2 A data sharing agreement has been established between the councils of North Yorkshire. The Multi-Agency Information Sharing Protocol (MAISP) group is also coordinating the review and update of other relevant information sharing agreements between the new council and external partners.

7.0 CYBER SECURITY

7.1 The impact of a significant cyber attack against the council as well as making systems unavailable could result in a significant data breach. The threat to local authorities continues as has been demonstrated previously and more recently with one council attacked for a second time. All these incidents have led to the loss of services to residents and potential data losses. It has been reported that the cost of recovery for one of these councils has been in excess of £10 million.

7.2 To mitigate this risk, the Technology and Change Service has invested in and continues to maintain several technical measures to minimise the likelihood of an attack and to reduce the impact if one occurs.

7.3 We proactively monitor for cyber threats through the use of security software and acting on intelligence received from trusted partner organisations e.g. National Cyber Security Centre (NCSC), Yorkshire & Humber Warning, Advice & Reporting Point (YHWARP) and Regional Organised Crime Unit (YHROCU). This monitoring has proved effective with the Information Security Team successfully identifying and blocking threat activity from various international locations.

7.4 As these measures cannot guarantee that the council will not fall victim to a cyber incident, our employees have an important role to play as the last line of defence. The Technology and Change Service therefore provides regular advice and guidance to them through training, intranet updates and key messages.

7.5 A revised set of training has been released to update employees on how to work securely. Regular simulations will also be carried out to improve their ability to identify phishing emails and to understand what actions they should take if they receive one.

7.6 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.

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 support one of the UK-GDPR requirements of storing data for 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 As we migrate emails and outlook into the Office 365 environment, other functionality within Office 365 will be rolled out to further improve our ability to manage information securely and effectively.

9.0 COVID-19 PANDEMIC

9.1 Privacy notices and data protection impact assessments have continued to be completed or amended as required in relation to the Covid-19 pandemic.

9.2 Work has been ongoing in relation to the Shielded Patient List/Clinically Extremely Vulnerable (CEV) data to ensure that data is being disposed of in line with legislation.

10.0 RECOMMENDATION

10.1 Members are asked to note the County Council’s information governance arrangements and activities 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

17 February 2022

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