NORTH YORKSHIRE COUNCIL

AUDIT COMMITTEE

24 JUNE 2024

INFORMATION GOVERNANCE ANNUAL REPORT

Report of the Corporate Director – Resources

1.0 PURPOSE OF THE REPORT

1.1 To provide an update on information governance matters, developments in the 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 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.

2.2 The 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 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 potential consequences should the Council suffer a serious data breach which, as well as regulatory action (including the possibility of financial penalties), the Council could suffer financial losses from data subjects seeking legal redress, and significant reputational damage.

3.0 **ROLES AND RESPONSIBILITIES**

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

Senior Information Risk Owner (SIRO)

The Corporate Director - 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 Council's management of information risks to Management Board and the Audit Committee. The Assistant Chief Executive - Legal & Democratic Services has been designated as the Deputy SIRO.

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 Council's Data Protection Officer.

Information & Cyber Security Team

The Information & Cyber Security team, hosted in the Technology Service, comprises three functions: Data Governance, Information Security and a Cyber Security Operations Centre ('Cyber SOC').

- The Data Governance team works with service areas to provide information governance and assurance; and supports the organisation in ensuring the quality and accuracy of its data. The team embeds information governance policies and shares information management best practice. This includes providing support with the preparation and maintenance of information asset registers, Data Protection Impact Assessments (DPIAs) and information sharing agreements. The team supports services to mitigate the risk of data breaches. The team also delivers relevant training to service teams and updates the mandatory data protection e-learning courses.

- The Information Security team works with service areas and Technology Service colleagues to identify, evaluate, and mitigate digital and physical information risks, and to achieve and sustain relevant information security compliance standards (e.g., ISO 27001). The team provides organisational guidance on access controls and permissions to the Council's ICT network,

technology infrastructure and ICT systems and applications. The team also delivers relevant training to service teams, including regular email phishing tests.

- The Cyber SOC team works with service areas and Technology Service colleagues to identify, evaluate and mitigate cyber threats, and to manage the organisational response to cyber incidents. The team researches, compiles, and acts on internal and external cyber intelligence with and from trusted partners. The team is focused on optimising organisational cyber resilience and embedding a swift and effective response to cyber security incidents.

Veritau Information Governance Team

As well as acting as Data Protection Officer, the Information Governance team within Veritau manages all Freedom of Information and Data Subject requests received by the Council. The team coordinates responses, provides general advice and guidance, reviews the application of exemptions, and responds to complaints concerning these legislative duties. 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, raises awareness of data protection obligations, and responds 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 the UK GDPR, 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 raising awareness of information governance responsibilities and good practice across the 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 Council.

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

- delivery of data protection impact assessment (DPIA) workshops
- delivery of data breach and data subject right of access training to specific teams within the Council
- reviewing and updating privacy notices as required
- reviewing any new agreements for supplies and services to ensure they properly reference the UK-GDPR
- working with relevant service areas in respect of any information sharing initiatives, to ensure all activity is being carried out in line with the relevant legislation

- consolidating County, District & Borough council record management responsibilities within the NYC Record Retention & Disposal Schedule (RRDS). The RRDS was also updated to reflect new local authority requirements arising from the UK Covid 19 inquiry and Independent Inquiry into Child Sexual Abuse (IICSA)
- updating internal processes and procedures in line with the Biometrics and Surveillance Camera Commissioners Code of Practice 2022
- engaging with the Information Commissioner's Office (ICO), Department for Digital, Culture, Media & Sport, and the technology sector to contribute to policy formation around the use of Artificial Intelligence (A.I.) and Machine Learning
- preparing for the possible future implementation of the Data Protection and Digital Information (DPDI) Bill, keeping informed of developments with the Bill and how it could possibly affect the Council.

5.0 DATA BREACHES

5.1 Council employees are required to report all information security incidents (personal 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 usually indicate a breach of procedure or policy, whilst increasing risk awareness; 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. Near miss incidents are where there has been a failure of security safeguards, but no breach of confidentiality, data integrity, or availability has actually taken place.

5.3 Starting in Q4 of 2023/24, Veritau has adapted its data breach report to exclude near misses from the main incident count. This has been done to ensure the report and key performance indicator better reflects the Council's management of the associated risks.

5.4 The number of reported personal data security incidents in the year to 31 March 2024 was as follows:

2023 / 24							
Quarter	**Very high**	**High**	**Moderate**	**Low**	**Very low**	**Total**	**Near Miss**
Q1	1	1	25	55	21	103	37
Q2	1	0	22	58	22	103	28
Q3	0	1	13	47	19	80	25
Q4	0	2	20	61	25	108	27
Total	**2**	**4**	**80**	**221**	**87**	**394**	**117**

5.5 The equivalent number of personal data security incidents reported in 2022/23, for North Yorkshire County Council was as follows:

2022 / 23							
Quarter	**Very high**	**High**	**Moderate**	**Low**	**Very low**	**Total**	**Near Miss**
Q1	0	1	7	38	13	59	17
Q2	0	1	15	28	18	62	29
Q3	0	0	12	34	24	70	28
Q4	0	1	14	43	22	80	35
Total	**0**	**3**	**48**	**143**	**77**	**271**	**109**

5.6 The corresponding data for the North Yorkshire district/borough councils is not fully complete so a direct comparison between years is not possible. However, the number of breaches now being reported for North Yorkshire Council appears consistent with the increase in service areas, employees and number of transactions since local government reorganisation. The reported breaches will continue to be monitored to identify any specific trends or issues.

5.7 6 data breaches were reported to the ICO in 2023/24, as follows:

Case Number	**Type of breach**	**ICO Decision (received)**
202300144	Incorrect document recipient	ICO responded with a No Further Action Decision (April 2023)
202300783	Unauthorised disclosure	ICO responded with a No Further Action Decision (June 2023)
202301465	Incorrect document recipient	ICO responded with a no Further Action Decision (January 2024)
202302027	Cyber incident – data processor	ICO Responded with no further actions, but shared advice in the form of "consideration" (October 2023)
202304450	Cyber incident – data processor	The ICO responded with the decision that regulatory action was not required (January 2024). The ICO provided the Council with advice on additional security, which is currently being reviewed

Case Number	Type of breach	ICO Decision (received)
202306158	Cyber incident	The ICO responded with the decision that regulatory action was not required (June 2024)

5.8 In previous years, information security has been highlighted as a significant control issue by the Head of Internal Audit and included in the Annual Governance Statement. The causes are varied but work is ongoing to reduce the frequency and impact of data breaches.

6.0 LOCAL GOVERNMENT REORGANISATION (LGR)

6.1 A significant amount of work was undertaken in 2022/23 to ensure that the new North Yorkshire Council would be compliant with the UK-GDPR and Data Protection Act 2018. This work has continued in 2023/24, and has included:

- embedding the Information Security Incident Process across the new Council to improve the awareness and reporting of incidents
- raising awareness of the Data Governance and Information Governance teams across the new Council to ensure better understanding of their respective responsibilities
- working with services to help provide a consistent approach to Data Protection compliance
- working with Brimhams Active to ensure the company's existing processes are compliant with data protection legislation. Further work will be undertaken to bring these processes in line with the Council's policy framework when the service is brought inhouse
- working with the Local Economic Partnership prior to its transfer into the York and North Yorkshire Combined Authority and supporting the establishment of the Combined Authority itself
- improving the Council's processes for managing requests for information. This has included running awareness campaigns, delivering a programme of training sessions across various service areas and hosting regular service/directorate meetings to help better coordinate responses.

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 the public sector continues with councils seeing an increase in the number of attempted attacks. Successful attacks 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 the councils affected in recent years was in excess of £10m.

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

7.3 The Council proactively monitors 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 & Cyber Security team successfully identifying and blocking threat activity from various national and international locations.

7.4 Due to the complex nature and realities of cyber-attacks, these technical measures cannot guarantee that the Council will not fall victim to a cyber incident, and our employees have an important role to play. The Technology Service therefore provides regular advice and guidance to staff 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 are also 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 Service continues 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 MICROSOFT 365 IMPLEMENTATION

8.1 As part of the Microsoft 365 implementation, the Council has delivered the ability to classify documents (email, word, excel etc) using the Government Security Classification Scheme (Official-Sensitive, Official, Not Protectively Marked). Classification has been improved to make it easier for the end user to understand and use, and where possible the classification is automated based on the content of the document.

8.2 We are also leveraging functionality within Microsoft 365 to categorise documents, allowing us to put in place retention and deletion 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 key document retention periods and to embed and automate this functionality within the Microsoft 365 environment.

8.3 We are in the process of developing a document migration strategy to identify, categorise and migrate all of the Council's legacy electronic and physical documents to Microsoft 365 or NYC Archives. This includes the identification and removal of ROT (Redundant, Obsolete and Trivial) information, which is no longer required, which may result in non-compliance with data protection legislation and is costly in terms of electronic storage. This strategy will make it easier for end users to find the information they need and will help expedite FOI and SAR information requests.

8.4 The above developments will enable us to start using Data Loss Prevention (DLP) within Microsoft 365, which will help reduce the likelihood of a serious data breach occurring. For example, DLP functionality can automatically block sensitive information being sent to a non-approved email address, or prevent a sensitive document from being unlawfully shared, edited or printed.

8.5 As we migrate emails and documents into the Microsoft 365 environment, other functionality will be rolled out to further improve our ability to manage information securely and effectively.

9.0 IMPLICATIONS

9.1 There are no local member, financial, human resources, legal, equalities or climate change implications.

10.0 RECOMMENDATION

10.1 Members are asked to note the Council's information governance arrangements and activities during the year.

Report prepared by Max Thomas, Head of Internal Audit (Veritau) and Greg Harper, Head of Information & Cyber Security (NYC)

GARY FIELDING
Corporate Director – Resources

County Hall
Northallerton

6 June 2024

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