NORTH YORKSHIRE COUNTY COUNCIL

AUDIT COMMITTEE

7 MARCH 2019

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
The General Data Protection Regulation (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 investigate 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 GENERAL DATA PROTRECTION REGULATION (GDPR) / DATA PROTECTION ACT 2018 (DPA)

4.1 The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) came into force in May 2018. A significant amount of work was undertaken to help prepare for the new legislation. CIGG monitored action plans and received regular updates on progress. Key actions completed or in progress include:

- Information Asset Registers are being prepared by each directorate. The registers identify all information assets and their associated information asset owners.
- Privacy notices are being prepared and published on the Council's website.
- The policy framework was reviewed and updated (see section 5 below).
- Training and guidance was provided to information asset owners.
- Contracts for supplies and services were reviewed to identify those involving the processing of personal information. A contract variation process has been developed and training provided to contract managers. The target is to complete all relevant contract variations by 30 June 2019.

5.0 POLICY FRAMEWORK

5.1 The following policies have been updated to reflect GDPR and DPA 2018, and approved by Management Board:

- Information Governance Policy Framework – Overview (IGP002)
- Information Transparency, Access, and Reuse Policy (IGP003)
- Data Protection Rights Policy (IGP004)
- Personal Privacy Policy (IGP005)
- Information Management Policy (IGP006)
- Information Security Overview (IGP009)
- Information Security Incident Management Policy (IGP011)

5.2 The Information Security Policy (PO 01) has been considered by CIGG and is now due to approved by Management Board. A Surveillance Policy (IGP007) has been drafted and will be presented to the next CIGG meeting for consideration. Work is also ongoing with the Social Media Acceptable Use (IGP008) and Information Security Classifications (IGP010) policies.

6.0 DATA BREACHES

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

6.2 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. Following the introduction of the new 'Information Security Incident (Data Breaches) Management' Policy, the County Council has started categorising some incidents 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).

6.3 The number of reported data security incidents since April 2017 is as follows:

Year	Quarter	Red	Amber	Green	White	Total
2017/18	Q1	1	14	5	0	20
	Q2	0	18	6	0	24
	Q3	3	10	10	0	23
	Q4	1	25	10	0	36
2018/19	Q1	3	30	9	3	45
	Q2	3	35	21	7	66
	Q3	3	34	21	6	64

6.4 Two data breaches have been reported to the ICO since 1 April 2018. In one case, the ICO decided to take no further action because it considered the risk of harm was low and the County Council had taken appropriate mitigating action. No response has yet been received from the ICO regarding the second case but, following investigation, the breach has been downgraded by the DPO.

7.0 CYBER SECURITY

7.1 The County Council completed a LGA self-assessment survey of its cyber security arrangements. This rated the Council's arrangements as Green. An action plan has now been prepared to address identified areas for improvement.

7.2 A number of test email phishing exercises have been completed during the year. The emails are designed to appear genuine and invite the recipient to click on a link and provide login details and passwords. Those employees who click on the link and go on to provide further information are identified. They are also redirected to a training site which explains the risks of phishing and provides further guidance on how to recognise suspicious emails.

7.3 The Technology & Change Service has maintained its certification of ISO 27001 which is an internationally recognised framework for Information Security ensuring that the Confidentiality, Integrity and Availability of data is maintained.

7.4 In an effort to ensure cyber security consistency across EU member states the European parliament adopted a 'Directive on Security of Network and Information Systems (NIS Directive)' which became enforceable in May 2018 to coincide with the introduction of the GDPR. Whilst the County Council is not classed as 'an operator of essential services', and therefore not directly compelled by the directive, it is likely that the Council may need to review and potentially update aspects of its cyber security arrangements to ensure compatibility when sharing data with partner agencies who are classed as operators of essential services (for example the police). The Council will work with partner agencies to ensure compliance with the directive's requirements.

8.0 SECURE DATA TRANSFER

8.1 The government's secure data network, Government Secure Internet, and the associated gcsx email domains will be discontinued as of 31 March 2019. The Council has implemented the required technical security changes to allow the normal @northyorks.gov.uk to be used for sending sensitive emails to other public sector bodies. The Council still has access to Egress where additional security is required for emails containing personal or confidential information which are sent to our residents and non-public sector bodies.

9.0 OFFICE MOVES / CONFIDENTIAL WASTE

9.1 A new 'audit' and authorisation process has been developed to improve the security of records where service teams are involved in office moves. This follows a number of data security incidents earlier in the last year. Veritau are checking some office moves to ensure the new process is being correctly followed.

9.2 Facilities Management has also reviewed and are improving processes for the collection of confidential waste. New locked confidential waste bins are due to be installed on the County Hall campus shortly.

10.0 RECOMMENDATION

10.1 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

5 February 2019

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