

AUDIT AND GOVERNANCE COMMITTEE

DATE	18 th April 2024
REPORT OF	Executive Director Place and Resources (S151)
SUBJECT	Information Governance and Security - Annual Governance Report
STATUS	Open

CONTRIBUTION TO OUR AIM

Effective information governance and security ensures the information we use and have access to is managed effectively, kept protected and secure, evidencing and informing decision making, forward planning and service delivery, and contributing to the achievement of the priorities and outcomes of the Council, the Place and our partners.

EXECUTIVE SUMMARY

This report outlines the key information governance and security activities undertaken by the Council in 2023 and provides assurance that the Council across all of its work areas and functions remains compliant with its legal obligations and follows good practice.

RECOMMENDATIONS

That the Annual information governance and security report for the calendar year 2023 at Appendix 1 be received and approved.

REASONS FOR DECISION

To support the Council's information governance activities.

1. BACKGROUND AND ISSUES

- 1.1 In order to carry out many of its' functions, the Council is required to process personal data and special category personal data about identifiable individuals (data subjects).
- 1.2 The UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018) set out the data protection principles that the Council must follow for the lawful, fair and transparent processing of personal data; as well as the rights that individuals have relating to the processing of their personal data to hold the Council to account and ensure that their privacy is respected. Failure to comply with these responsibilities can result in a monetary penalty of up to 20 million Euros (18 million pounds) or 4% of global annual turnover.
- 1.3 Other information governance legislation that must be complied e with when processing personal data, include the Privacy and Electronic Communications Regulations, the Human Rights Act, Freedom of Information Act, Environmental Information Regulations and associated Codes of Practice.

Failure to comply with these legal obligations, can result in:

- a) Inconvenience, distress, prejudice or harm to individuals or organisations.
- b) Loss or compromise of personal, commercial, or sensitive data affecting the Council's ability to make decisions and / or deliver services.
- c) Damage to the Council's reputation which may result in a loss or reduction in the level of trust others have in us.
- d) Enforcement action and / or a monetary penalty from the Information Commissioner's Office, and / or
- e) Prosecution through the Courts.
- f) Loss of the ability to take card payments in person or online
- g) Restricted access to the Public Services Network

1.4 Common factors in the cause of many data and cyber incidents are human error and a lack of awareness of responsibilities and good practice.

1.5 To address these risks and raise awareness, understanding and compliance with our obligations, policies, procedures and guidance for the effective management and security of personal data and associated systems are in place, and promoted at both corporate and service levels, supported by mandatory data protection and cyber security training for all staff (including agency staff and partners accessing the Council's network) and Elected Members.

2. RISKS AND OPPORTUNITIES

Ineffective information governance and security arrangements have a number of inherent risks in the context of organisational management, the use of resources and service delivery. Addressing the issues raised in the report is a means of mitigating such potential risks and maximising opportunities for effective information management and security to support decision making and service delivery.

3. OTHER OPTIONS CONSIDERED

None.

4. REPUTATION AND COMMUNICATIONS CONSIDERATIONS

Each of the issues identified in the annual information governance and security report could have a potential reputational impact if not addressed.

5. FINANCIAL CONSIDERATIONS

Not applicable in relation to this report.

6. CLIMATE CHANGE AND ENVIRONMENTAL IMPLICATIONS

There are no such implications arising from this report.

7. FINANCIAL IMPLICATIONS

There are no financial implications arising directly from this report. However we need to continue to be mindful of the potential financial implications arising as a result of failure to comply with council policies, standards and statutory legislation.

8. LEGAL IMPLICATIONS

The Council is under a duty to ensure that it processes, holds and releases any information in line with a range of legislative provisions including the UK General Data Protection Regulation, Data Protection Act 2018, Freedom of Information Act, Privacy and Electronic Communications Regulations and the Human Rights Act. The Council also has a duty to publish information wherever possible, and in accordance with its own publication scheme. However, regard should be had to not publishing any information of a confidential or sensitive nature, in accordance with the relevant legislation and public interest tests.

9. HUMAN RESOURCES IMPLICATIONS

There are no human resource implications arising directly from this report. However we need to continue to be mindful of the potential employee relations' implications arising as a result of failure to comply with council policies and standards.

10. WARD IMPLICATIONS

All wards.

11. BACKGROUND PAPERS

None.

12. CONTACT OFFICER(S)

Paul Ellis, Strategic Lead Business Practice and Performance (Data Protection Officer), Tel 01472 32 3372

John Padley, Cyber Security Technical Specialist, Tel 01472 326123

Joanne Robinson, Assistant Director Policy Strategy & Resources, (Deputy Senior Information Risk Owner) Tel 01472 323761

Sharon Wroot
Executive Director Place and Resources (S151)
Senior Information Risk Owner

Appendix 1

Annual Information Governance Report for the calendar year 2023

1 Introduction

- 1.1 The purpose of this report is to update the Audit and Governance Committee on the Council's information governance (IG) and security activities and provide assurance of its compliance with its legal obligations.

2 Information Governance and Security arrangements

- 2.1 The Council has officers appointed to the following information governance and security roles: Senior Information Risk Owner, Deputy Senior Information Risk Owner, Caldicott Guardians, Deputy Caldicott Guardian, Data Protection Officer, Cyber Security Technical Specialist, Clinical Safety Officer, and Information Asset Owners. In 2023, the Council increased its Caldicott Guardians arrangements from one to three, with specific individuals identified for Adult Social Care, Children Social Care and Public Health.
- 2.2 Through an Information Security and Assurance Board (ISAB) the Council reviews and maintains its information governance, management and security arrangements, policies and procedures reflecting local lessons learnt, developing good practice and changes to legislation and codes of practice.
- 2.3 The Council's cyber security arrangements are managed through a specialist team within the ICT and Digital service.
- 2.4 Cyber and IG risks are included on the Corporate Risk Register and are reviewed and updated as a standing agenda item of the ISAB. As part of the assessment of risk in relation to the processing of data in 2023, 29 stage 1 and 11 stage 2 Data Protection Impact Assessments were completed.
- 2.5 Assurance activities include reviews with Information Asset Owners of the Record of Processing Activity Register, Corporate Retention Schedule and Information Sharing Agreement Register, and information governance risk and compliance reviews for each of the Council's buildings with the building responsible person.
- 2.6 In 2023 the Council maintained its compliance with the Public Services Network Code of Connection and the NHS Data Security and Protection toolkit.
- 2.7 The North East Lincolnshire Archives are managed on our behalf through Lincs Inspire and are accredited through The National Archives.
- 2.8 We work proactively with place and regional partners (including the Humber and North Yorkshire ICB) to ensure a collaborative and consistent approach to information governance, management and security compliance and promotion and are members of the Yorkshire and Humber Public Sector Network, the

Humber Information Governance Alliance, Yorkshire and Humber Information Governance Group, Strategic Information Governance Network and the North East Lincolnshire Caldicott Guardian's Group.

3 Mandatory information governance training and awareness raising

- 3.1 The 6th data protection principle states personal data shall be processed in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures ('integrity and confidentiality').
- 3.2 An essential part of this is raising awareness and understanding of the importance of keeping personal data protected and secure, the responsibilities for this and the legislation, policies, procedures, and standards in place to support this. Everyone acting on behalf of the Council has a personal responsibility for ensuring the information they process is kept protected and secure, and when logging on to the Council's ICT network, users are required to confirm compliance with the Council's policies and standards.
- 3.3 All officers and elected members with access to the Council's ICT network must complete the mandatory 'Cyber Awareness and Staying Safe Online' and the 'Data Protection: Compliance Following GDPR' e-learning modules as part of their induction and refresh this annually. ICT Officers with privilege accounts are required to complete the Privilege Users Terms of Use Agreement.
- 3.4 For officers without access to the Council's ICT network, awareness is raised through the 'Keep It Safe' leaflet and a requirement to sign a declaration confirming they understand their responsibilities.
- 3.5 Officers and their Line Managers are automatically notified through the Learning Management System when they are required to undertake their training, with additional reminders issued if not completed within one month. Currently 98% of officers are compliant with their induction / refresher GDPR training, and 91% compliant with their Cyber Awareness training.
- 3.6 Compliance details are available to line managers in real-time, with ISAB receiving a list of outstanding officers on a weekly basis to chase up non-compliance, with procedures in place to suspend the network access of any officer who does not complete the training within the agreed timescales.
- 3.7 To support our Caldicott Guardian arrangements a training session was provided by Member of the UK Caldicott Guardian Council, with spare places made available to local and regional partners.
- 3.8 Awareness raising at officer, service, corporate and place level of information governance, management and security issues and good practice, is further supported and embedded through internal Wiki pages, intranet / YAMMER staff communications postings, email updates, articles in Vision (employee newsletter), workshops, and specific support to individuals, services, and

projects.

- 3.9 During 2023, there has been a continued focus on maintaining and raising awareness of Cyber Security reflecting the increased risk and sophistication of phishing and cyber-attacks. Dedicated campaigns have taken place to target every person with network access with a phishing simulation email.

4 Incidents and breaches reported in 2023

- 4.1 Arrangements are established for the reporting of data incidents, which are allocated to an investigating officer and reported to the Information Security and Assurance Board for review and sign off. These arrangements continue to be reviewed to ensure lessons are identified and improvements made to policies, procedures and controls. The ICT and Information Security Policy and a Wiki page on the staff intranet provide guidance on the reporting and investigation of incidents.

- 4.2 In 2022, 173 incidents were investigated, a slight increase on the previous year. Corresponding figures for the previous 5 years are:

Calendar Year	Incidents	Reported to the ICO
2023	173	5
2022	156	5
2021	148	3
2020	120	1
2019	124	9
2018	87	5

- 4.3 The continued increase in and the number of incidents can likely be attributed to officers being more aware of the need to report all data incidents through our mandatory training, awareness raising activities and guidance, even relatively minor incidents such as emails going to the wrong internal recipient or post being sent to a former address and returned to the Council unopened, which may not have been reported previously.

- 4.4 The investigations identified that for 154 of the incidents there was negligible or a managed risk to the data subject, and 10 found that no data breach had occurred. 1 was found to be third party incident, for 3 insufficient information was provided to allow an investigation to take place and 1 incident was reported twice.

- 4.5 4 incidents were self-reported to the Information Commissioner's Office (ICO), who determined that no further action was necessary.

- 4.6 A further 1 incident was reported to the ICO by the data subject. The ICO determined no further action was necessary on this occasion but recommended that the Council conducted further investigation into the causes of the incident,

to ensure that the cause was fully understood and that further steps were taken to prevent it from happening again.

5 Handling of Access to Information requests

5.1 In 2023, 1,187 Freedom of Information requests were received, of which 95% were responded to within 20 working days. 16 internal reviews were requested concerning the handling of the requests, of which 1 was escalated to the ICO for independent resolution. This complaint is currently being investigated by the ICO, who are considering whether or not the Council holds the requested information.

5.2 Corresponding figures for the previous 5 years are:

Calendar Year	Requests	responded to in 20 days	Internal reviews	ICO complaints
2023	1,187	95%	16	1
2022	1,083	94%	27	2
2021	1,010	94%	23	6
2020	1,092	82%	12	4
2019	1,418	96%	19	3
2018	1,433	96%	24	3

5.3 2023 volumes are slightly high than the previous 3 years, but lower than the volumes received pre Covid, no reason can be directly attributed for this reduction of pre 2020 figures.

5.4 The percentage of requests responded to within the statutory timescale of 20 working days, at 95%, continues to show recovery from the reduced level of 82% in 2020 which is attributed to the reallocation of resources for service delivery as part of the COVID-19 working arrangements.

5.5 In 2023, we received 61 Subject Access Requests and 123 third party information requests processed under the Data Protection Act, in 2022 we received 43 and 122, respectively.

5.6 To improve the efficiency of the redaction process and ensure that information redacted from documents cannot be re-identified redaction software is now in use across the Council.

6 Internal Audits

6.1 The following internal audits related to IG have been issued.

- ICT Remote Access (NELC), March 2023 — Audit Assurance: Satisfactory & Risk: Low
- ICT Disaster Recovery (NELC), March 2023 — Audit Assurance: Satisfactory & Risk: Medium
- ICT Cloud computing Follow up (NELC), September 2023 — Audit Assurance: Substantial & Risk: Medium

- ICT - Inventory Management (NELC), January 2024 — Audit Assurance: Satisfactory & Risk: Low

6.2 The following audits are scheduled this year:

- Information Governance
- Customer Service System
- ICT strategy overview
- Income system

6.3 It should also be noted that non-IG and security related audits may include reviews of IG and security controls and practices.

7 Future Actions

7.1 ISAB will continue to monitor and review our information governance and security arrangements including policies, procedures, guidance, and training (both current provision and future need) to ensure compliance with our statutory duties and promote officer understanding. This monitoring and review will reflect any developments or changes required as a result of the reforms to the UK's data protection regime and identified good practice.

7.2 Monitoring of the completion of the mandatory e-learning modules for Cyber Security and Data Protection against agreed deadlines will continue, with appropriate action taken against those not complying.

7.3 Awareness raising activities will continue with a specific focus on cyber security and phishing attacks.

7.4 To provide assurance of information governance compliance to ISAB and the Senior Information Risk Owner a review of the Record of Process Activity Register, Corporate Retention Schedule and the Information Sharing Agreement Register with Information Asset Owners is scheduled for April 2024, with Building Information Governance Checks with the responsible person for the building planned for June 2023.

7.5 Work will continue with partners to develop a consistent and collaborative approach for information management and security for the place of North East Lincolnshire and the wider region. Discussions are taking place with the North Bank Forum to provide information governance support and training for our voluntary, community or social enterprise partners.

7.6 The Council will continue to meet all compliance requirements and conduct annual penetration testing.

Sharon Wroot
Executive Director Place and Resources