AUDIT AND GOVERNANCE COMMITTEE

DATE	21st April 2022
REPORT OF	Executive Director of Environment, Economy and Resources (S151)
SUBJECT	Information Governance and Security - Annual Governance Report
STATUS	Open

CONTRIBUTION TO OUR AIM

Effective information governance ensures the information we use and have access to is managed effectively, kept protected and secure, evidencing and informing decisions 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 activities undertaken by the Council in 2021 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 Report for the calendar year 2021 at Appendix 1 be received and approved.

REASONS FOR DECISION

To support the Council's information governance activities.

1. BACKGROUND AND ISSUES

1.1 The Council in order to carry out many of its functions and satisfy legal obligations is required to process personal data and special category personal data about identifiable individuals (data subjects).

1.2 When processing personal data, the Council must comply with its legal obligations (including the UK General Data Protection Regulation (GDPR), Data Protection Act 2018 (DPA 2018), Freedom of Information Act, Privacy and Electronic Communications Regulations and the Human Rights Act) and associated Codes of Practice.

1.3 In May 2018, data protection legislation in the United Kingdom and the European Union changed. In the UK, the Data Protection Act 1998 was replaced by the EU GDPR and the DPA 2018, expanding the rights of individuals with regards to the processing of their personal data, introducing greater safeguards on the processing of personal data ensuring the privacy of individuals is respected and making those processing personal data more accountable and transparent. Failure to comply can now result in an increased monetary penalty of up to 20 million Euros (18 million pounds) or 4% of global annual turnover.

1.4 Following the end of the Brexit transition period on 31 December 2020, the EU GDPR no longer applied in the UK. However, the UK's DPA 2018 has enacted the EU GDPR's requirements into UK law, and with effect from 1 January 2021, the UK data protection regime is set out in the DPA 2018 and the UK GDPR. In June 2021, the EU made an adequacy decision in relation to the UK.

1.5 To ensure we understand and comply with our obligations, policies, procedures and guidance for the effective management of personal data are in place at both corporate and service levels, supported by training and awareness activities.

1.6 Failure to comply with these policies and standards, could result in the following outcomes:

a) Inconvenience, distress, prejudice or harm to individuals or organisations affected.
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.

1.7 Each individual member of staff has a personal responsibility for ensuring the information they process is kept protected and secure. When logging on to the Council's ICT network, users are required to confirm compliance with the Council's policies and standards.

1.8 A common factor in the cause of many data incidents is a lack of awareness of data protection responsibilities and good practice. To address this, there is a mandatory requirement for all staff (including agency) and Elected Members to undertake data protection and cyber security training.

2. RISKS AND OPPORTUNITIES

Ineffective information governance 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 Annual Information Governance report is a means of mitigating such potential risks and maximising opportunities for effective information management and use 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 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 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

Effective information governance is relevant to all wards.

11. BACKGROUND PAPERS

None.

12. CONTACT OFFICER(S)

Paul Ellis, Head of Information Governance & Complaints (Data Protection Officer), Tel 01472 32 3372

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

Sharon Wroot
Executive Director of Environment, Economy and Resources (S151 Officer)
Senior Information Risk Owner

Appendix 1

Annual Information Governance Report for the calendar year 2021

1 Introduction

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

2 Information Governance and Security arrangements

2.1 The Council has officers in the following IG roles: Senior Information Risk Owner, Deputy Senior Information Risk Owner, Caldicott Guardian, Deputy Caldicott Guardian, Data Protection Officer, Advanced Practitioner – Cyber Security, Clinical Safety Officer, and Information Asset Owners.

2.2 Through an Information Security and Assurance Board (ISAB) the Council review and maintain its information governance, management and security arrangements, policies and procedures reflecting local lessons learnt, developing good practice and changes to legislation and standards.

2.3 Cyber and IG risks on the Corporate Risk Register 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 2021 16 Stage 1 Data Protection Impact Assessments were completed and 37 Stage 2 assessments.

2.4 As part of the Information Governance internal audit a review has taken place of the Record of Processing Activity Register, Retention Schedule and Information Sharing Agreement Register.

2.5 The arrangement for the technical information security function delivered through the shared service with North Lincolnshire Council ended on March 31st, 2021. The Council now have sole responsibility for its technical information security, which is managed through a dedicated officer, the Advanced Practitioner – Cyber Security.

2.6 In 2021 the Council again achieved 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 through Lincs Inspire and are accredited through The National Archives.

2.8 Through the Council / CCG Union arrangements, opportunities for efficiencies from a consistent approach, coordination of activities and the reduction of duplication are maximised. This includes the development of common or harmonised policies, supporting procedures and standards, training and awareness raising materials, and security products across both networks.

2.9 Opportunities with place and regional partners for a collaborative approach for information governance, management and security compliance and promotion are actively progressed through the Yorkshire and Humber Public Sector Network, the Humber Information Governance Alliance, Yorkshire and Humber Information Governance Group, Humber Coast and Vale Health and Care Partnership, Strategic Information Governance Network and the North East Lincolnshire Caldicott Guardian's Group.

2.10 To ensure that our cyber security arrangements continue to meet the ever developing and sophisticated threat of phishing and cyber-attacks a Cyber Security Audit is planned for 2022, and the use of sensitivity labelling is being explored, which will to enforce data loss prevention.

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 ensuring everyone is aware of and understand the importance of keeping personal data protected and secure, their responsibilities for this and the legislation, policies, procedures, and standards in place to support this.

3.3 All officers and elected members must complete the mandatory Cyber Awareness and Staying Safe Online and the Data Protection: Compliance Following GDPR e-learning module annually.

3.4 For officers without access to the Council's ICT network, awareness is raised through the Keep It Safe leaflet and a requirement that they sign a declaration confirming they understand their responsibilities.

3.5 The mandatory training was relaunched in October 2021, as part of the new Learning Management System.

3.6 Compliance details are available to line managers in real-time, monitored by the ISAB on a monthly basis, with procedures in place to suspend the network access of any officer who does not complete the training within the agreed timescales.

3.7 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 Wiki pages, intranet postings, email updates, articles in Vision (employee newsletter), workshops, and specific support to individuals, services, and projects.

3.8 During 2021, there has been a focus on maintaining and raising awareness of Cyber Security reflecting the increased risk and sophistication of phishing and

cyber-attacks. A number of different communication methods have been utilised for this, including the weekly Leadership message from the Chief Executive, 'Vision' staff magazine, and messages on the Intranet such as the 12 Days of Cyber Christmas. There has also been a focus on risks and good practice when home working, which included a survey of officers that asked questions about data protection and IG compliance that attracted 1,244 responses from staff.

.

4 Incidents and breaches reported in 2021

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 sign off. These arrangements continue to be reviewed to ensure lessons are identified and improvements made to policies, procedures and controls. A Wiki page is in place on the staff intranet to provide information about the reporting and investigation of incidents.

4.2 In 2021, 148 incidents were investigated, an increase on the previous year, which can be attributed to the increased awareness of officers and members of the public to report potential incidents. Corresponding figures for the previous 5 years are:

Calendar Year	Incidents	Reported to the ICO
2016	43	3
2017	38	6
2018	87	5
2019	124	9
2020	120	1
2021	148	3

4.3 The investigations identified that for 130 of the incidents there was negligible or a managed risk to the data subject, 12 found that no data breach had occurred, and for 3 there was insignificant evidence to enable an investigation to take place.

4.4 3 incidents were self-reported to the Information Commissioner's Office (ICO), who determined that no further action was necessary.

4.5 A further incident was reported to the ICO by the data subject in relation to historic data processing arrangements, who determined that as a result of weaknesses in the arrangements in place in 2007, an infringement of data protection law had occurred.

4.6 Normally during the year information compliance spot checks are undertaken in each of the Council's buildings, to identify any IG risks and raise user awareness to assist in the prevention of data incidents. Due to COVID restrictions these checks did not take place in 2021, to address this guidance

and good practice has been issued to officers to support home / agile working to ensure that information and equipment is kept protected and secure.

4.7 The building compliance checks recommenced in February 2022.

5 Handling of Access to Information requests

5.1 In 2021, 1,010 Freedom of Information requests were received, of which 81.9% were responded to within 20 working days. 23 internal reviews were requested concerning the handling of the requests, of which 6 were escalated to the ICO for independent resolution.

5.2 Historically we would expect to receive circa 1,400 requests each year. 2021 like 2020 has seen a reduction of circa 20% on previous years which based on the available evidence is likely to be attributed to COVID-19.

5.3 Normally over 95% of requests are responded to within the statutory timescale of 20 working days. In 2021 the figure is 94%, recovering from the reduced level of 82% in 2020 which was attributed to the reallocation of resources for service delivery as part of the COVID-19 working arrangements.

5.4 Corresponding figures for the previous 5 years are:

Calendar Year	Requests	responded to in 20 days	Internal reviews	ICO complaints
2021	1,010	94%	23	6
2020	1,092	82%	12	4
2019	1,418	96%	19	3
2018	1,433	96%	24	3
2017	1,285	97%	12	0
2016	1,244	97%	43	12

5.5 42 Subject Access Requests and 129 third party information requests processed under the Data Protection Act were also received during the calendar year of 2021.

6 Internal Audits

6.1 The following internal audits related to IG were issued in 2021/22

- Information Governance (Audit Assurance: Satisfactory - Risk: Low) actions updated and implemented.
- ICT Controls HR Payroll Application (Audit Assurance: Satisfactory - Risk: Low)
- ICT Project Management Controls Follow Up (Audit Assurance: Limited - Risk: Medium)
- ICT Solution Centre (Audit Assurance: Substantial - Risk: Low)
- Income (Audit Assurance: Substantial - Risk: Low)

6.2 It should also be noted that non-IG related audits may include reviews of IG

controls and practices.

6.3 Audits are currently being undertaken on the following, and will be reported on in the Annual Report for 2022

- Cloud computing
- Cyber crimes
- Disaster recovery
- eFinancials
- ICT Controls new Finance system
- Remote Access
- Web accessibility and transparency

7 Future Actions

7.1 ISAB will continue to develop, maintain, promote and monitor the arrangements, policies, procedures, standards, training needs and activities of the Council to ensure compliance with statutory IG duties. This will include any developments / changes as a result of the UK Government consultation “Data: A new direction” and looking at opportunities to improve the handling of access to information requests.

7.2 To continue to work 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 linking to the new Humber and North Yorkshire Integrated care partnership which replaces the Humber, Coast and Vale Health and Care Partnership and brings together the six CCGs.

7.3 Continue the monitoring of the mandatory e-learning modules to ensure that all officers complete their Cyber Security and Data Protection training within agreed deadlines.

7.4 To complete the information compliance building checks, ensuring compliance with Council arrangements for the protection and security of the information we hold and the working environment, and identify opportunities for improvement.