AUDIT AND GOVERNANCE COMMITTEE

DATE	22nd April 2021
REPORT OF	Executive Director of Environment, Economy and Resources
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 2020 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 2020 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 General Data Protection Regulation, Data Protection Act 2018, Freedom of Information Act, Privacy and Electronic Communications Regulations and the Human Rights Act) and associated Codes of Practice. 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.

1.3 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 General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (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 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.

1.5 Following the end of the Brexit transition period on 31 December 2020, the EU GDPR no longer applies 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.

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 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 information 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 year 2020

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 Through the Information Security and Assurance Board (ISAB) the Council review and maintain its information governance, management and security policies and procedures reflecting local lessons learnt, developing good practice and changes to legislation and standards; ensure appropriate training is available for officers; and raise IG awareness at officer, service, corporate and place level.

2.2 The IG risks on the Corporate Risk Register are reviewed and updated as a standing agenda item of the ISAB.

2.3 The technical information security function in 2020 was delivered through the shared service with North Lincolnshire Council (Northern Lincolnshire Business Connect). This arrangement 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).

2.4 As part of the Council / CCG Union, the Council and the CCG have a joint Data Protection Officer in place.

2.5 Through these arrangements opportunities for efficiencies and cost reductions 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.

2.6 North East Lincolnshire Archives are managed through Lincs Inspire and are accredited through The National Archives.

2.7 For 2020 the Council again achieved compliance with the Public Services Network Code of Connection and the NHS Data Security and Protection toolkit.

2.8 A collaborative approach for information governance, management and security compliance and promotion across the Humber region is coordinated through the Humber Information Governance Alliance (HIGA), a network of IG professionals from the public and private sector including local authorities, Fire and Rescue Service, NHS bodies and the Police. The members of HIGA include organisations from the wider Humber, Coast and Vale Health and Care

Partnership.

2.9 A North East Lincolnshire Caldicott Guardian's meeting takes place with representatives from the Council, CCG, Care Plus Group, Focus, NAVIGO, NLAG and Saint Andrew's Hospice.

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 that staff should be 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 There is a mandatory requirement for staff processing health data to complete an e-learning module on data protection and security annually, with all other staff required to complete the module every two years.

3.4 For staff 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 August 2020, since when over 95% of officers have completed their induction / refresher training including all staff processing health data. Arrangements are in place for the outstanding officers (new starters, long term absence and unused casual employees) to complete their training.

3.6 Compliance is reported on monthly, and procedures are in place to suspend the network access of any officer who does not complete the training within the agreed timescales.

3.7 Awareness raising of information governance, management and security issues and good practice, is further supported and embedded through presentations / workshops, email updates, intranet postings, Wiki pages, articles in Vision (employee newsletter) and specific support to individuals, services and projects. During 2020, there has been a focus on raising awareness of the risks and good practice for home working, this has included the development of new guidance and Wiki pages.

3.8 Following participation in the LGA's Cyber Security Stocktake, £5,000 grant funding was received towards an email phishing simulation tool – PurplePhish, launched in December 2019.

3.9 Email phishing attacks are becoming increasingly common and more

sophisticated. To raise employee awareness of them and assist in the detection and prevention of them, all employees were enrolled onto the 12-month Cyber Security Awareness Training programme, consisting of a series of Phishing Simulations, a short educational video and quiz each month.

4 Incidents and breaches reported in 2020 (1st January - 31st December)

4.1 Arrangements are established for the reporting of data incidents, these 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 to provide information about the reporting and investigation of incidents.

4.2 In 2020, 113 incidents were investigated, a slight decrease on the previous year. Corresponding figures for the previous 5 years are:

Year	Incidents	Reported to the ICO
2015	42	2
2016	43	3
2017	38	6
2018	87	5
2019	124	9
2020	113	1

4.3 The investigations identified that for 96 of the incidents there was negligible or a managed risk to the data subject with a further 16 it was found that no data breach had occurred.

4.4 Only 1 incident met the criteria requiring reporting 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, who determined that the Council had complied with its data protection obligations, as there was a legal obligation to disclose the information.

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 have been unable to take place, but guidance and best practice has been issued to officers to support home / agile working to ensure that information and equipment is kept protected and secure.

5 Handling of Freedom of Information request

5.1 In 2020, 1,092 Freedom of Information requests were received, of which 81.9% were responded to within 20 working days. 12 internal reviews were requested concerning the handling of the requests, of which 4 issues were escalated to the ICO for independent resolution.

5.2 Normally each year 1,400 requests are expected to be received, for 2020 there has been 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, this figure has reduced during COVID-19 as resources were concentrated on service delivery. The backlog of requests has now been tackled and the number of outstanding and out of time requests reduced.

5.4 Corresponding figures for the previous 5 years are:

Year	Requests	responded to in 20 days	Internal reviews	ICO complaints
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
2015	1,223	95%	49	3

6 Internal Audits

6.1 The following internal audits related to IG were issued in 2020/21

- Data Quality (Audit Assurance: Satisfactory - Risk: Low)
- Information Governance (Audit Assurance: Satisfactory - Risk: Low)
- Finance System Resilience Audit (Audit Assurance: Substantial - Risk: Low)
- Human Resources and Payroll System Resilience (Audit Assurance: Satisfactory - Risk: Medium)

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

7 Future Actions

7.1 The Information Security and Assurance Board continue to develop, maintain, promote and monitor the policies, procedures, standards, training needs and activities of the Council to ensure compliance with statutory duties; embed corporate awareness and understanding; identify and mitigate risks; and maximise opportunities for improvement in the area of information management and security.

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 wider Humber, Coast and Vale region.

7.3 To progress recommendations and actions from the Information Governance Internal Audit with a particular focus on the review of the Record of Processing Activity Register and the Retention Schedules.

7.4 Continue the monitoring of the mandatory Information Governance training to ensure that all officers complete their induction / refresher training.

7.5 Information compliance spot checks will recommence as soon as restrictions allow. Work has also commenced on exploring opportunities to further raise awareness of good practice / expected behaviours whilst working agilely and how compliance and understanding can be tested.

7.6 Following the end of the Brexit transition period, the Council will continue to monitor the implications and requirements of the UK being considered a third country for the purpose of data transfers with the EU.