AUDIT AND GOVERNANCE COMMITTEE

DATE 23rd July 2020

REPORT OF Director of Resources and Governance

SUBJECT Information Governance and Security - Annual Governance Report

STATUS Open

CONTRIBUTION TO OUR AIMS

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 2019 and provides assurance that the Council across all work areas and functions remains compliant with its legal obligations and follows good practice.

RECOMMENDATIONS

That the Annual Information Governance Report for 2019 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 its functions and satisfy legal obligations is required to process personal data and special categories of personal data about identifiable natural persons (data subjects).

1.2 When processing personal data, the Council must comply with the requirements of legislation (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 On May 25th, 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 and the Data Protection Act 2018, increasing the rights of individuals with regard 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 Failure to comply with these policies and standards, could result in the following outcomes:

a) Inconvenience, distress or prejudice 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 or a monetary penalty from the Information Commissioner's Office, and / or
e) Prosecution through the Courts.

1.6 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

Paul Hudson, ICT Shared Services Group Manager (Deputy Senior Information Risk Owner) Tel 01472 32 3977

Sharon Wroot
Director of Resources and Governance (Chief Finance Officer)
Senior Information Risk Owner

Appendix 1

Annual Information Governance Report for the year 2019

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 activities, policy, procedures and standards

2.1 Through the Information Security and Assurance Board the Council review and maintain its information governance, management and security policies and procedures to reflect 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 As part of the Council / CCG Union, the Council and the CCG have a joint Data Protection Officer in place. The technical information security function is delivered through the shared service with North Lincolnshire Council (Northern Lincolnshire Business Connect). 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.

2.3 Information compliance spot checks were undertaken in each of the Council's buildings, to identify any IG risks and raise user awareness.

2.4 In 2019 the Council again achieved compliance with the Public Services Network Code of Connection and the NHS Data Security and Protection toolkit, which replaced the NHS Information Governance toolkit.

2.5 North East Lincolnshire Archives which are managed through Lincs Inspire are accredited through The National Archives. This status is provisional, and its retention depends on the satisfaction of additional requirements by July 2020.

2.6 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. During 2019, HIGA has invited organisations from the wider Humber, Coast and Vale STP to attend.

2.7 HIGA links to the Humber Local Digital Roadmap Board and has supports their

work on the NHS Local Health and Care Record Exemplar programme for Yorkshire and Humber which aims to develop shared health and care records at a regional level building on existing local arrangements.

2.8 The IG risks on the Corporate Risk Register are reviewed and updated as a standing agenda item for the Information Security and Assurance Board.

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.

3.3 For staff without access to the Council's ICT network, awareness is raised through a leaflet with a requirement that they sign a declaration confirming they understand their responsibilities.

3.4 In 2019 all 165 staff processing health data completed the annual training. As at 06/01/2019, 1387 staff had successfully completed the e-learning module and 308 staff had received the leaflet and signed the declaration. 11 members of staff were still to complete the training, who fell into the category of new starters, those on long term absence and casual employees.

Completed e-learning module	1,387	81.30%
Received leaflet and signed declaration	308	18.05%
Total completed training	1,695	99.35%

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

3.6 Awareness raising of information governance, management and security issues and good practice, is further supported and embedded through presentations / workshops, email updates, intranet postings, articles in Vision (employee newsletter) and specific support to individuals, services and projects.

3.7 In 2019, an Information Management Wiki section was created with pages on Remote working; Data incident reporting; Freedom of Information; Retention

and Disposal; Mandatory training; Subject Access Requests; and Telephone and Video calling.

4 Incidents and breaches reported in 2019 (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. In 2019, a Wiki page was created to provide staff with information about reporting incidents and the investigation report template was updated.

4.2 In 2019, 124 incidents were reported and investigated. This is an increase on previous years and reflects the increased awareness of staff in the handling of personal data and the potential risks, as well as increased awareness of data subjects seeking clarity on the use of their personal data.

4.3 Corresponding figures for the previous 5 years are:

Year	Incidents	Reported to the ICO
2019	124	9
2018	87	5
2017	38	6
2016	43	3
2015	42	2
2014	47	0

4.4 The investigations identified that for 92 of the incidents there was negligible risk to the data subject and a further 23 it was found that no data breach had occurred.

4.5 Nine data protection incidents were reported to the Information Commissioner's Office (ICO), who determined that:

a) For 6 of the reported incidents no further action was necessary;
b) 1 incident, reported by the data subject, did not constituted an inappropriate disclosure;
c) 1 incident concerning a third party, was not a reportable breach; and
d) 1 incident, which related to an allegation of unlawful obtaining of personal data committed against the Council, should be allocated to the ICO's Criminal Investigation Team.

4.6 A further incident was reported to the ICO by the data subject, who determined that the Council had complied with its data protection obligations.

5 Handling of Freedom of Information request

5.1 In 2019, 1,418 Freedom of Information requests were received, of which 96% were responded to within 20 working days.

5.2 19 internal reviews were requested concerning the handling of the requests, of which 3 issues were escalated to the ICO for independent resolution.

5.3 Corresponding figures for the previous 5 years are:

Year	Requests	responded to in 20 days	Internal reviews	ICO complaints
2019	1418	96%	19	3
2018	1433	96%	24	3
2017	1285	97%	12	0
2016	1244	97%	43	12
2015	1223	95%	49	3
2014	1451	95%	76	6

6 Internal Audits

6.1 The following internal audits related to IG were issued in 2019/20

- General Data Protection Regulations Assessment (Satisfactory Assurance / Low Risk)
- Assurance Audit of Network Device Security and Management Controls (Satisfactory Assurance / Low Risk)
- Liquidlogic Children's Management System IT General Controls (Satisfactory Assurance / Low Risk)
- Direct Debits for Green Waste (Advisory audits do not give a traffic light opinion score.)

6.2 An Information Governance audit is schedule for 2020/21 – 2021/22, with an initial outline of policies are embedded in the day to day operations and are compliant with legislation and national guidance; employees and members are made aware of the framework; processes are in place to ensure policies are followed; and effective processes are in place to manage records and information.

6.3 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 will continue on behalf of the Council 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. Specific activities include:

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.

7.3 To progress actions and manage risks identified in internal audits, spot checks and incident investigations.

7.4 In 2019, NELC received funding following participation in the LGA's Cyber Security Stocktake involving all 353 English Councils. The results from this questionnaire developed bespoke reports for each Local Authority which enabled NELC to apply for grant funding in areas identified were improvement could be made. NELC received grant funding of £5,000 towards an email phishing simulation tool - PurplePhish.

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 have been enrolled onto a 12 month Cyber Security Awareness Training programme. The training consists of a series of Phishing Simulations, a short 2-3 minute educational video and quiz each month.