Report of the Director: Governance and Communities

Meeting 13 July 2022

NORTH LINCOLNSHIRE COUNCIL

AUDIT COMMITTEE

ANNUAL INFORMATION GOVERNANCE UPDATE

1. OBJECT AND KEY POINTS IN THIS REPORT

1.1 To provide the Audit Committee with an annual position statement on the council's Information Governance arrangements.

1.2 The key points are:

- The council is required by law to comply with a range of information related requirements.
- Further developments have taken place over the last 12 months to strengthen the council's approach to Information Governance. Details are set out in the report together with the findings from internal and external assessments.

2. BACKGROUND INFORMATION

2.1 An assurance report is presented to the Audit Committee each year to provide an update on the council's information governance arrangements and associated compliance.

2.2 The council has a legal obligation to comply with information legislation, notably the UK General Data Protection Regulation (UK GDPR)/Data Protection Act 2018, Freedom of Information Act and the Environmental Information Regulations. Collectively we refer to these requirements as "information governance".

2.3 An Information Governance Framework comprising a series of individual policy schedules sets out how the council will comply with legislation and good practice. Its implementation is led and overseen by the Data Protection Officer with support from the Senior Information Risk Owner.

2.4 The council is committed to the ongoing strengthening of its Information Governance arrangements and continues to strive to meet the standards set by both internal audit and external assessments, with a high standard of compliance evidenced as summarised below.

2.5 Key developments and assurance highlights over the last 12 months included:

- The annual Information Governance Self-Assessment, necessary for accessing health information, would usually have been completed by 31 March, but due to the COVID19 pandemic the submission date for 2021 was deferred by the NHS to 30 June 2022. The council's submission was submitted on-time and it is anticipated that it will be accepted by the NHS as meeting all relevant standards.

- An internal audit review of the council's approach to compliance with the UK General Data Protection Regulation (GDPR) and Data Protection Act 2018 concluded in June 2021 with a "satisfactory assurance / medium risk" opinion. Further progress has been made to meet the requirements

- The information governance policy framework was comprehensively reviewed and updated in March 2021 and again in July 2021 and January 2022 to align it with changes in legislation and latest professional practice.

- Training for all employees on information governance requirements, including the UK GDPR, is undertaken on a regular basis and forms part of the council's mandatory training suite.

- The annual communication campaign was undertaken in August 2021 as a refresher for all employees of key data protection considerations. The 2022 campaign is planned for Quarter 3 of 2022.

- A new business system was introduced in 2021 to manage the work flowing of information requests such as Freedom of Information (FOI), from their receipt through to approval and issue. This improved the visibility of the status of individual information requests and overall monitoring of processing performance and has been expanded during 2022 to cover wider information governance enquiries.

2.6 Each year the council handles hundreds of information requests and processes hundreds and thousands of customer transactions. During the last 12 months, to the end of May 2022, there have been four referrals from the Information Commissioner's Office (ICO) about how the council responded to requests for information or protected personal information. This number is lower than the previous year where there were five referrals and is within the normal reporting levels/business parameters. In addition, the council self-reported three issues to the ICO. The findings were as follows:

- The action taken by the council for a referral case from the previous year was supported by the ICO and the case closed.

- In respect of the three self-reported issues, the ICO supported the council's approach in two cases and required no further action.

- As of end of May 2022 we are awaiting a response from the ICO on the third case. The outcome will be reported to the audit committee in future reports.

2.7 Compliance with national ICT security standards was maintained and externally certified with no serious ICT breaches occurring in the last year. Key highlights are set out below:

- In January 2022, the council achieved 'Cyber Essentials' certification which helps to guard against the most common cyber threats and demonstrates our commitment to cyber security.

- Attempted email phishing attacks are becoming increasingly common nationally and more sophisticated. To raise employee awareness and assist in the detection and prevention of such attacks, all employees have been enrolled for a further year to the "Boxphish" 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.

- A series of external tests are completed each year by expert third parties to test the strength of the council's IT security arrangements. In addition, an ongoing relationship is maintained with regional and national cyber security centres to share information on threats and mitigation measures.

- The council participated in the Local Government Association (LGA) Cyber 360 programme with the main aim to support councils working to reduce cyber risk, build cyber capabilities and improve the understanding of cyber security principles across the organisation.

- In June 2021 the council's IT arrangements were certified as compliant with the national Public Services Network (PSN) Code of Connection. This certification provides the council with continued access to wider public service networks such as Department for Work and Pensions and NHS. The same assurance has been sought for 2022 but is still going through the assessment process.

2.8 Further continued strengthening of the council's information governance and cyber security arrangements will be made over the next 12 months through an ongoing action planning based approach.

3. OPTIONS FOR CONSIDERATION

3.1 As set out below.

4. **ANALYSIS OF OPTIONS**

4.1 **Option 1 –** The Audit Committee agrees that the current position provides sufficient assurance in our approach to Information Governance.

4.2 **Option 2 –** The Audit Committee considers the current position is not sufficient and requests that additional work is undertaken.

5. **FINANCIAL AND OTHER RESOURCE IMPLICATIONS (e.g. LEGAL, HR, PROPERTY, IT, COMMUNICATIONS etc.)**

5.1 Not applicable.

5.2 An integrated impact assessment is not required for this report.

6. **OTHER RELEVANT IMPLICATIONS (e.g. CRIME AND DISORDER, EQUALITIES, COUNCIL PLAN, ENVIRONMENTAL, RISK etc.)**

6.1 There are no other relevant implications.

7. **OUTCOMES OF INTEGRATED IMPACT ASSESSMENT (IF APPLICABLE)**

7.1 An integrated impact assessment is not required for this report.

8. **OUTCOMES OF CONSULTATION AND CONFLICTS OF INTERESTS DECLARED**

8.1 There are no consultations or conflicts of interests to report.

9. **RECOMMENDATIONS**

9.1 The Audit Committee should consider whether the report provides sufficient assurance of the adequacy of the council's Information Governance arrangements.

DIRECTOR: GOVERNANCE AND COMMUNITIES

Church Square House
SCUNTHORPE
North Lincolnshire
DN15 6NL
Author: Phillipa Thornley, Data Protection Officer
Date: 27 June 2022

Background Papers used in the preparation of this report
As referred to in the main body of the report