Joint Report of the Director:
Governance and Partnership and
Director: Business Development

Agenda Item No: 10
Meeting: 27 June 2018

NORTH LINCOLNSHIRE COUNCIL

AUDIT COMMITTEE

ANNUAL INFORMATION GOVERNANCE AND ICT SECURITY UPDATE JUNE 2018

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 and ICT Security Functions.

1.2 Key points are:

- The council are required by law to comply with a range of information related requirements such as Data Protection legislation.
- An Information Governance and ICT Security Policy Framework is in place to support the council in complying with legislative requirements.
- The council has undertaken a number of internal and external assessments, which indicate assurance in its operation of these functions.

2. BACKGROUND INFORMATION

2.1 An annual assurance report is presented to the Audit Committee in June of each year detailing the current position of the council's Information Governance and ICT Security arrangements.

2.2 Since June 2017 further improvements have been made to the Information Governance and ICT security frameworks primarily in readiness for the new General Data Protection Regulation (GDPR).

2.3 The implementation of the GDPR that came into force on 25 May 2018 to replace the Data Protection Act 1998. Significant work was undertaken to prepare the council for the change in legislation. An external audit has taken place on our readiness for GDPR resulting in satisfactory assurance with low risk.

2.4 At the end of March 2018, the sixth NHS Information Governance Self-Assessment was made and accepted at the level required to maintain the council's access to certain health information.

2.5 Successfully completed the council's first joint Public Services Network (PSN) Code of Connection through the shared service, aligning both council's submissions dates and associated activities.

2.6 In September 2017, the annual IT Security Health Check was carried out as part of our PSN compliance application. All security remediation actions were completed or mitigating controls applied where remediation was not possible.

2.7 We successfully received our annual PSN compliance certificates in May 2018 without qualification or challenge from the assessor for both Councils.

2.8 An external audit found that our approach to PSN compliance provided satisfactory compliance with low risk.

2.9 A campaign to raise awareness of Information Governance good practice has been produced and rolled out. This comprised of six weekly council wide messages, an electronic booklet containing all messages and a week-long screen saver.

2.10 New mandatory council wide employee training has been launched to cover Information Governance and IT Security.

2.11 Listed below are other ICT Security enhancements that have been made over the past year:

- Implemented Government Secure Email to replace the legacy GCSx secure email which includes:
- encrypting email in transit over the internet between government organisations using Transport Layer Security (TLS);
- Implemented technical and business policies to check inbound and outbound government email to avoid our domains being used fraudulently (e.g. for spam or spear-phishing).
- Procured a new Penetration Testing Partner to carry out our IT Health Checks
- Promoting the use of secure email and continuing to raise cyber security awareness across the council.
- Strengthened our Microsoft patching policy to fix any known security bugs

2.12 Awareness of the importance of information request legislation is reported via a monthly performance report to Head of Service. The report includes Freedom of Information and Environmental Information Regulation requests and the purpose is to maintain appropriate council response times in line with legislative requirements. This has continued to have a positive impact and has further improved our response time in line with our statutory duty.

2.13 Data Protection Impact Assessment (DPIA) are being put together where high risk processing of personal information is carried out and going forward must be carried out where there is a high risk to individuals in relation to personal information, such as where new ICT is being introduced that could affect privacy.

2.14 The use of the Corporate Records Store at Glanford House has carried on being embedded into council process and the recent further rationalisation of buildings has seen additional records placed into storage there. Security has been enhanced at the facility. Considerations are now being given to storing some or all records in electronic format.

3. OPTIONS FOR CONSIDERATION

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

4. ANALYSIS OF OPTIONS

4.1 The report identifies the required compliance in respect of Information Governance requirements and ICT Security requirements and provides an update as to the areas of development to ensure continued compliance and improvement in these areas.

5. RESOURCE IMPLICATIONS (FINANCIAL, STAFFING, PROPERTY, IT)

4.1 Not applicable.

6. OUTCOMES OF INTEGRATED IMPACT ASSESSMENT (IF APPLICABLE)

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

7. OUTCOMES OF CONSULTATION AND CONFLICTS OF INTERESTS DECLARED

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

8. RECOMMENDATIONS

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

DIRECTOR: GOVERNANCE AND PARTNERSHIP
DIRECTOR: BUSINESS DEVELOPMENT

Civic Centre
Ashby Road
SCUNTHORPE
North Lincolnshire
DN16 1AB

Author: Phillipa Thornley/Paul Smith
Date: 11 June 2018