ITEM 12

NORTH YORKSHIRE COUNTY COUNCIL

AUDIT COMMITTEE

2 March 2017

INFORMATION GOVERNANCE – PROGRESS REPORT

Report of the Corporate Director – Strategic Resources

1.0 PURPOSE OF THE REPORT

1.1 To update Members on the progress made to further develop the County Council's Information Governance arrangements.

2.0 BACKGROUND

2.1 Since 2010, the County Council has had a comprehensive policy framework covering all aspects of Information Governance (IG). Significant work has been undertaken since then in order to raise awareness of the policy requirements and ensure compliance. Information is a key asset for the Council (like money, property, or the skills of its staff) and must be protected accordingly. Much has been achieved in this area but there is a continuing need to maximise compliance and embed a culture of sound information governance, particularly in relation to information security.

2.2 According to the Terms of Reference of the Audit Committee, its role in respect of information governance is:

(i) to review all corporate policies and procedures in relation to Information Governance

(ii) to oversee the implementation of Information Governance policies and procedures throughout the County Council

2.3 Information governance remains a high risk area as identified on the Corporate Risk Register. This is, in part, due to the ever increasing risks in a hi-tech environment and the behavioural challenges encountered. The current view is that this will be an area of on-going high risk despite the Council's actions to mitigate those risks.

3.0 STRATEGIC OVERVIEW AND PRIORITISATION OF WORK

3.1 In September 2016 the Corporate Information Governance Group carried out a review of the objectives set out in the Information Governance Policy and Strategy to enable better realignment with the current priorities for information governance. The outcome of the exercise is that the Group will now focus on the following areas:

- Information Asset Registers
- Information Security and Transferring Information Securely
- Training and Changing Culture
- Data Sharing with Partner Agencies

This has enabled the work to be more focused on these particular areas however other issues are included when required and it is appropriate to do so.

4.0 INFORMATION ASSET REGISTERS

4.1 An Information Asset Register (IAR) is a working reference document for identifying and organising information assets. It should be used to identify governance and risk issues affecting each item, such as sensitive, or sensitive personal, data; retention and deletion periods, data sharing and most importantly the Information Asset Owner responsible for managing those risks.

4.2 Recent guidance and best practice from the Information Commissioners Office and Local Government Association on recording and managing information assets in an IAR has been considered, and an updated template with categories of information has been produced to take this into account. A full review and refinement of existing Directorate and Service IARs will take place over the next 4 months to ensure compliance with the updated requirements.

4.3 Once the registers have been updated, training and support will be targeted at those IAOs responsible for those information assets which represent the greatest risk (for example, where personal sensitive data is routinely shared with partners).

4.4 As previously mentioned, IARs are regarded as a working document subject to change to reflect new and emerging risks, changing priorities and/or service developments. Review of IARs will therefore be on going and be subject to change as we gain a better understanding of the cross-cutting risks and priorities.

5.0 INFORMATION SECURITY COMPLIANCE

Information Security Compliance Checks

5.1 Internal Audit has been carrying out unannounced compliance audits relating to information security for some time. Out of the 6 audits that have been carried out in the past year, 5 have been classified as ‘Limited Assurance’. Examples of non-compliance include:

- Sensitive data relating to children and adults being left unsecured, such as SEN review lists, school admission forms, details of health and wellbeing, individual placement agreements, clients’ files and lists containing other personal details.
- Sensitive data relating to staff being left unsecured, such as interview and application forms, staff supervision, disciplinary and appraisal files, and photocopies of passports.

- Security related information, such as usernames and passwords, safe codes and bank account details
- Unsecured laptop and other electronic devices, and keys.

5.2 Where non-compliance has been identified this has been brought to the attention of the relevant managers promptly with appropriate remedial action taken as necessary. Details of non-compliance have also been reported to the Corporate Information Governance Group (CIGG) and directorate information governance champions so as to help develop further guidance, training and other awareness raising measures. Information security is now regularly considered by directorate management teams and a number of services have instigated their own ongoing compliance checks.

5.3 There are also examples of good practice such as at Thirsk Highways Area Office where the audit was classified as 'High Assurance'.

Data Security Incidents

5.4 97 data security incidents were reported in the first 9 months of 2016/17. All reported incidents are investigated with the most serious ones being referred to Internal Audit. The majority of these incidents have been caused by human error. Typical examples include:

- Documents sent to incorrect recipients by email or post (often because information recorded on systems was not updated and address or email details were not properly verified);
- Documents containing personal information left in unsecure locations;
- E-mail recipients addresses disclosed because the blind copy function was not used;

5.5 The number of incidents has increased significantly since the last report. On the surface this may not be seen as a positive sign but it does indicate that there is heightened awareness of the issues. Staff are encouraged to quickly flag breaches and data security incidents so that recovery arrangements can be made and lessons subsequently learned. It is accepted that human error will never be eradicated but care and attention is essential when handling sensitive data. For this reason, work is ongoing to raise awareness, provide guidance and the necessary tools (for example secure e-mail facilities) and test compliance.

Information Commission Office Self Referrals

5.6 Although there is no legal obligation on data controllers to report breaches of security which result in loss, release or corruption of personal data, the Information Commissioner believes serious breaches should be brought to the attention of his Office. The nature of the breach or loss can then be considered together with whether the data controller is properly meeting his responsibilities under the Data Protection Act. 'Serious breaches' are not defined however, data controllers consider the potential detriment to data subjects together with the volume and sensitivity of personal data involved in deciding whether breaches should be reported.

5.7 During the last year, the Council has self-reported 3 data breaches to the Information Commissioner's Office. One of these reports was subsequently withdrawn as further investigations showed that it was not as serious as initially thought. The other 2 referrals were investigated by the Information Commissioner's Office which concluded that the Council's actions and planned actions following the breaches were appropriate.

6.0 TRAINING AND CULTURE

6.1 Training and changing the culture of the employees of the organisation in relation to information security continues to be challenging. This is not because employees maliciously jeopardise the security of information but more as a result of human error and lack of care and attention when handling sensitive data. This is demonstrated in **paragraph 5.4 on Data Security Incidents** above.

Mandatory Training

6.2 There has been mandatory training in place for some time. The 3 in depth mandatory online learning courses have recently received a minimal refresh. Posts required to carry out the 3 in depth courses have been identified and this includes the majority of employees in the Council.

6.3 For other employees that are not required to carry out in depth training because they do not routinely manage sensitive data, there is an Introduction to Handling Information. This forms part of the induction process for an employee. A refresher course is being developed to follow on from the introductory course

6.4 The online courses have helped employees to understand their responsibilities in relation to personal and sensitive information. However, further discussions about the training framework and how we update existing training are taking place. This is to help ensure that the connection between the training and the application of the knowledge learnt by employees continues to increase. Work is being scheduled with some "high risk" teams on IG matters to determine if there are practical actions that can be taken to help teams to minimise the risks of error. There is therefore a balanced approach being pursued to push compliance.

Phishing Trial

6.5 As with any organisation the Council is under constant threat of cyber-attack and one of the most common is a phishing email. Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons. If a user's credentials are provided to a real phishing email there are a number of outcomes. One outcome could be the Council email details are used to send spam. This could lead to the Council email address '@northyorks.gov.uk' being blacklisted. If this happens it means that emails sent by Council users may not be received by the intended recipient impacting on service delivery.

6.6 The Council has systems in place to reduce the number of these phishing emails that get into an email inbox. However, to identify any further potential weakness relating to phishing e mails that do manage to enter an email inbox, an email of the type often used by hackers was created and sent to a sample of email accounts.

6.7 This exercise has helped to highlight where further support and training on this subject is required. There will be further phishing email exercises carried out in the future to test the effectiveness of the support and training provided and will hopefully show an improvement in user awareness and behaviour.

7.0 DATA SHARING WITH PARTNER AGENCIES

7.1 There is a need for the Council to share information with a variety of external partners. Whether this is between social care and health, District Councils or the Police, the information governance requirements and standards that have to be adhered to are the same.

7.2 It is accepted that there is already a great wealth of information sharing practice happening within the council and externally with key partners. However, there is also a need to align our processes to ensure we are sharing information appropriately, at the right time, with the right people and by the correct means.

7.3 In response to this, a collaborative Multi Agency Overarching Information Sharing Protocol (the “Protocol”) has been produced. The Protocol helps to create a positive culture of sharing information and facilitate more effective data sharing practices between partner agencies, with the ultimate aim of improving service delivery and resident outcomes. Refusing to share data can be a risk just as much as sharing too much data.

7.5 The Protocol applies to all information being shared by signatory partner agencies, with the aim of establishing the types of data which these agencies will share, how data is handled and the legislation which allows the information to be shared, and outlining processes for developing individual Information Sharing Agreements.

7.6 The majority of key partners in North Yorkshire have signed the Protocol, however there are still some organisations which have been identified as potential signatories. Discussions are ongoing with these.

8.0 RECOMMENDATIONS

8.1 Members are asked to note the progress made on information governance issues.

GARY FIELDING
Corporate Director – Strategic Resources

County Hall
Northallerton

March 2017

Authors of report: Fiona Sowerby, Corporate Risk and Insurance Manager and Max Thomas, Head of Internal Audit
Tel 01609 532400 and 01609 532143

Background papers: None