Leeds
CITY COUNCIL

Report author: Andrew Nutting and Terry Booth

Tel: 07891 276168

Report of Assistant Chief Executive (Customer Access and Performance)

Report to Corporate Governance and Audit Committee

Date: 22nd April 2013

Subject: Annual Information Governance Report

Are specific electoral Wards affected? If relevant, name(s) of Ward(s):	☐ Yes	☒ No
Are there implications for equality and diversity and cohesion and integration?	☒ Yes	☐ No
Is the decision eligible for Call-In?	☐ Yes	☒ No
Does the report contain confidential or exempt information? If relevant, Access to Information Procedure Rule number: Appendix number:	☐ Yes	☒ No

Summary of main issues

1. The report provides a summary brief of work being undertaken to ensure the Council is in the best position to mitigate against the threat of future information security breaches.

2. The report outlines progress being made in delivering information governance training across the organisation, together with information about resource and capacity to deliver information governance initiatives across the organisation.

3. The report provides an overview of the Information Commissioner's decision to issue a monetary penalty notice and undertaking on the council in December 2012.

4. The report details progress made by IT Services to implement a range of technologies to improve security across the Council.

5. This report provides Committee Members with assurances about the on-going work across the council to mitigate against the risk of future information security incidents, although it should be noted that this will not provide the council with a guarantee of security breaches not happening in the future. The conclusion of this report, identifies that whilst the range of information technologies deployed across the council's IT estate over the last five years provides Committee with relatively good assurance about protecting electronic information assets against cyber attack and security mishaps, on-going work is required to improve information handling practice across the council to

reduce the risk to hardcopy information. This report outlines measures being introduced to improve all types of information handling, including a strategy for training staff on information governance matters.

Recommendations

6. Corporate Governance and Audit Committee is asked to consider the contents of this report and the assurances provided as to the Council's approach to information security.

1 Purpose of this report

1.1 To provide Corporate Governance and Audit Committee with an annual report on the steps being taken to improve Leeds City Council's information security in order to provide assurance for the annual governance statement.

2 Background information

2.1 Leeds City Council recognises the need to protect its information assets from both accidental and malicious loss and damage. Information security is taken very seriously by the council and this is evidence by the on-going work to improve the security of our information as outlined in this report.

2.2 The report provides Committee Members with an update on the more strategic and cross-council activity on-going to provide assurance on our approach to information security. In this regard it covers actions taken to address the policy framework and development, information governance training, skills and competencies and the technology requirements within the organisation.

2.3 This year's report additionally provides Committee Members with an outline of the incidents that led to the intervention by the Information Commissioner and the steps being taken to help prevent similar incidents occurring in the future.

3 Main issues

Framework and Policy Development

3.1 The council's Information Governance Framework sets out the strategic plan for the organisation to ensure that appropriate arrangements are put in place to protect the council's information assets and reputation. The Framework was reviewed in 2012 and the Information Governance Management Board approved minor changes to its content at its meeting on 13th November 2012. The Information Governance Framework is underpinned by fourteen key policies, which enable the council to meet its legal, regulatory, contractual and business obligations. These policies are listed below:

- Information Security Policy;
- Data Protection Policy;
- Information Sharing Policy;
- Information Risk Management Policy;
- Information Security Risk Management Policy;
- Information Systems Acceptable Use Policy;
- Protective Marking and Asset Control Policy;

- Freedom of Information & Environmental Information Regulations Policy;
- Records Management Policy;
- Remote Access Policy;
- Clear Desk and Clear Screen Policy;
- Removable Media and Mobile Computing Policy;
- Records Retention and Disposal Policy;
- Data Quality Policy.

3.2 The policy on Information Risk Management was approved on 25th October 2012, which means all policies have been approved. It is the intention of the council to ensure information risk management is embedded into business processes and functions, in a very practical manner that is both scalable and proportionate in the way it is applied. To this extent a framework of supporting work is to be developed for this purpose and this will be aligned with the council's corporate risk management policy and procedures.

3.3 To support the implementation of information risk management measures and to mitigate against future information security incidents, the council is implementing a range of solutions aimed at providing secure methods of information handling. A blended solution for secure email accounts has been introduced, which has led to a reduction in implementation costs for services. A corporate process is being developed for deployment of secure email accounts to all those service areas identified as high risk, including those in Adult Social Care and Children's Services. Some deployment of secure email accounts to these high risk service areas has already happened, with the remainder expected to take place during the first two quarters of 2013/14.

3.4 Members of Governance and Audit Committee will be aware from previous reports that the council intends to deploy the Government Protective Marking Scheme (GPMS) as an information security classification system. This is to ensure that the council is able to share sensitive data with other public authorities through secure solutions. A tactical technical solution has been procured that will automate the labelling of secure markings on documents and emails is to be piloted within three service areas. This will provide a comprehensive evaluation of the product, before an implementation to secure email account holders and consideration of changes to GPMS descriptors proposed by the Cabinet Office for July 2013.

3.5 During 2012 a procedure for reporting information incidents was successfully implemented across the council to support the Information Incident Management policy. Each Directorate across the council and each of the ALMO's have an Information Compliance Officer who is trained to investigate incidents involving the council's information assets. A quarterly report about information incidents occurring across the council is provided to the council's Senior Information Risk Officer and the Information Governance Management Board. Furthermore, a review of the incident management process is to take place early in 2013/14, to evaluate a stricter interpretation of an information incident and examine how the council's Disciplinary Procedure can be consistently applied to staff involved in the most serious information incidents.

Information Governance Policy Training

3.6 In order to embed information governance practice it is recognised that the council's workforce will need to undertake training, and the degree and regularity of this training will depend, in part, to the type of information being processed. Members will be aware from last year's report that the information governance training programme consists of three levels:

- Level One – Mandatory basic training on information governance policies – e-learning for PC users, receipt of a brochure for non-PC users;

- Level Two – builds on the Level One training, is classroom based, face-to-face and interactive. It provides staff with a high level of understanding about appropriate data handling;

- Level Three - will comprise bespoke training, briefings and development sessions delivered to services which have been identified as high risk by Information Compliance Officers.

As at 26th March 2013, 94% of council staff have undertaken Level One training. This figure excludes ALMO staff, who are conducting a separate training programme on information governance. Work on Level One training is on-going to ensure staff who have been on long term absence are captured and to drive up the compliance rate to as close to 100% as is possible.

3.7 Level Two training has been piloted in Revenues and Benefits, Business Support and with Student Social Workers and feedback about training content has been favourable and positive. A programme to rollout this training is being developed, but priority will be given to those service areas identified as high risk.

3.8 Where a need is identified to provide more specific information governance training, bespoke training will be developed and delivered. For example, this may be determined through delivering level two training that staff require more focused information governance training, or, training is required to deliver part of the information governance programme such as the delivery of GPMS.

3.9 A dedicated officer with requisite training skills and experience has been appointed on a two year fixed term contract to develop and deliver information governance training.

3.10 In June 2012 Members Management Committee approved a recommendation to offer Members information governance training. To this extent Members will be invited to attend a series of workshops to be held in April and May 2013 that will help to improve their understanding about managing and sharing information in a safe and secure way.

Skills and Competencies

3.11 In addition to providing a framework of best practice, there is also a need to ensure the council has the relevant expertise in place to support the provision and implementation of effective policies and approaches regarding information security.

3.12 An information governance resource now exists in each Directorate of the council and is engaged with implementing aspects of the Information Governance Framework. Children's Services have now completed a review and have a full complement of information governance resources. Adult Social Care have strengthened their information governance capacity by engaging an Information and Knowledge Management manager to coordinate information governance activities in relation to the integration with Health. The appointment of an Information Governance manager within the ALMO's Business Centre Limited as provided assurance that the council's information governance policies will be implemented across the three ALMO's and BITMO.

3.13 Whilst there is an information governance resource within each Directorate, arrangements vary within each Directorate and it continues to be difficult to provide assurance about the consistency to the delivery and implementation of the Information Governance Framework across the council. However, an assessment of how information governance is currently delivered and scope for future requirements is being reviewed as part of the Enabling Corporate Centre review and the Business Management Programme. The views of the corporate Information Governance team about how information governance can be delivered across the organisation more effectively and efficiently are being fed into both projects.

3.14 A member of Corporate Leadership Team has been identified and trained to act in the capacity of the council's Senior Information Risk Officer (SIRO). This meets Local Government Association guidance about local authorities have a SIRO at board level. The SIRO will play a fundamental role in shaping the council's information risk management environment and is responsible for advising the Chief Executive about risks associated with the council's information assets. The SIRO is a member of the newly formed West Yorkshire SIRO Group, which meets quarterly to discuss the practicalities of providing a consistent approach to managing information risk within public authorities across West Yorkshire.

The Information Commissioner's Issuing of a Monetary Penalty Notice and Undertaking on the council

3.15 Members of this Committee will be aware that the ICO served a Monetary Penalty Notice on Leeds City Council on 16th November 2012 in respect of documents containing sensitive personal information being sent to a wrong recipient from within Children's Services and issued the Chief Executive with an Undertaking as a result of a breach of security to the Leeds Initiative website. Both incidents were reported to the ICO in July 2011.

3.16 Following the incident, Children's Services have implemented remedial measures to militate against a similar incident occurring again, and the Information

Governance Management Board has approved similar measures being adopted across the council. A project to ensure all council contracts with third parties meet data protection requirements is underway across the council. The council is confident that the requirements listed in the ICO's Undertaking will be met in full. Furthermore the exercise is providing the opportunity to review all existing contracts and ensure appropriate information governance requirements form part of the contract. Moving forward, information governance requirements will form essential criteria in the council's new procurement management framework.

Technology

3.17 The past year has been dominated by the Essential Services Programme (ESP), the most visible part of which is the deployment of Windows 7 and Office 2010 onto the desktop. However, within the Essential Services Programme there have been a number of developments which maintain or improve the council's technical security:

- There have been a completed refresh of the council's DMZ (Demilitarised Zone) which has seen the replacement of technology approaching the end of its life with more up to date technology;

- Microsoft Unified Gateway has been deployed, giving us ways of better securing our services to staff, partners and the public from outside the council;

- Microsoft Active Directory and 'NetApp' storage have been implemented which gives us the capability to better control access to stored information;

- We have brought forward 'Actividentity' tokens to replace the existing Vasco tokens. These are more flexible, cost effective and can be used in more different ways than the Vasco tokens, plus they are more secure;

- Windows 7 has security features as standard; a key feature is the ability to encrypt the hard disks of laptops. With Windows XP,we had to purchase and install encryption software separately. Windows 7 will save time and money whilst maintaining our levels of security.

3.18 The past year has been dominated by the Essential Services Programme (ESP), the most visible part of which is the deployment of Windows 7 and Office 2010 onto the desktop. However, within the Essential Services Programme there have been a number of developments which maintain or improve the council's technical security.

3.19 There has been a completed refresh of the council's DMZ which has seen the replacement of technology approaching the end of its life with more up to date technology;

3.20 Microsoft Unified Access Gateway has been deployed, giving us ways of better securing our services to staff, partners and the public from outside the council;

3.21 Microsoft Active Directory and ‘NetApp’ storage have been implemented which gives us the capability to better control access to stored information;

3.22 We have brought forward ‘ActivIdentity’ tokens to replace the existing Vasco tokens. These are more flexible, cost effective and can be used in more different ways than the Vasco tokens, plus they are more secure;

3.23 Windows 7 has security features as standard; a key feature is the ability to encrypt the hard disks of laptops. With Windows XP, we had to purchase and install encryption software separately. Windows 7 will save time and money whilst maintaining our levels of security.

3.24 The council has been implementing an Electronic Document and Records Management System (EDRMS) for Business Support Centre as part of Phase One development, but due to the supplier going into receivership, the council is currently re-assessing its options around how EDRMS can be best deployed across the council.

4 Corporate Considerations

4.1 Consultation and Engagement

4.1.1 Consultation on the development of all information governance policies, procedures and standards are extensively undertaken across a broad range of stakeholders including information management professionals, representatives from all Directorates, Trades Unions and Information Governance Management Board members.

4.2 Equality and Diversity / Cohesion and Integration

4.2.1 Equalities, diversity, cohesion and integration are all being considered as part of delivering the Information Governance Framework. This refers to the way training is being delivered as well as how the policies will impact on staff and partners.

4.3 Council policies and City Priorities

4.3.1 The policies support the Information Governance Framework and contain areas of legal requirement. Furthermore, the implementation of the Information Governance Framework will improve the quality of the council’s Policy Framework by ensuring the authenticity, integrity and security of the information contained therein.

4.3.2 Under the Code of Corporate Governance in Part Five of the council’s Constitution, the fourth principle (taking informed and transparent decisions which are subject to effective scrutiny and risk management) requires decision making processes and enables those making decisions to be provided with information that is relevant, timely and gives clear explanation of technical issues and their implications.

4.4 Resources and value for money

4.4.1 Capacity within Directorates to deliver, embed and monitor compliance to the information governance policies and practice is required, and resources for this are deployed from existing FTE's within Directorates and capacity is continually monitored by the Corporate Information Governance Team.

4.4.2 The way Information Governance is structured and organised is being reviewed as part of the Enabling Corporate Centre project with a view to improving the way information management is deployed and delivered across the organisation and city.

4.5 Legal Implications, Access to Information and Call In

4.5.1 There are no legal implications from this report.

4.5.2 There are no restrictions on access to information contained in this report.

4.6 Risk Management

4.6.1 The risk associated with not implementing information governance policies, procedures and practice across the Council leaves the organisation more susceptible to breaches of legislative, regulatory and contractual obligations, affecting the confidence of its citizens, partners, contractors and third parties when handling and storing sensitive and protectively marked information.

4.6.2 The risk of not deploying the range of technologies already commissioned to secure the Council's information assets leaves the organisation vulnerable to malicious attacks on its IT network infrastructure and exposes information assets to unnecessary security risks.

5 Conclusions

5.1 Information Governance has rightly been identified as a key area of risk and is being addressed through the implementation of improved policies, procedures and practice, training and technology. The range of Information Technology products implemented across the council over the past five years provides the council with relatively good assurance that it can protect its electronically held information assets. The nature of information incidents suggest that further work is required to embed information governance policies into council processes and practice, and that on-going training is required to educate staff in respect of handling council information.

5.2 Work will continue over the next twelve months to continue and extend the range of training, develop an information risk management framework and monitor compliance with policies. These measures will help to mitigate the council against future security threats and incidents.

6 Recommendations

6.1 Corporate Governance and Audit Committee is asked to consider the contents of this report and the assurances provided as to the Council's approach to information security.

7 Background documents[1]

None

[1] The background documents listed in this section are available to download from the Council's website, unless they contain confidential or exempt information. The list of background documents does not include published works.