Leeds CITY COUNCIL

Originator: Andy Nutting

Tel: 07545 604251

Report of the Assistant Chief Executive (Policy, Planning and Improvement)

Corporate Governance and Audit Committee

Date: 17th March 2010

Subject: Annual Information Security Report

Electoral Wards Affected:	**Specific Implications For:**
	Equality and Diversity ☐
	Community Cohesion ☐
☐ Ward Members consulted (referred to in report)	Narrowing the Gap ☐

Executive Summary

Breaches of information security and losses of data, both nationally and at a local level, have focused the attention of the Council to become more accountable for technical failures or for the contravention procedures which lead to the loss or disclosure of sensitive information.

Through the development of an Information Governance Framework, Leeds City Council is looking to ensure that its information assets are processed, stored and exchanged with partners in a safe and secure manner. It is important that the Council's citizens, business partners and staff have confidence and assurances that sensitive information is processed and dealt with securely.

Furthermore, the national agenda for transformational government and shared services has placed an additional emphasis upon the Council to ensure that it has fit for purpose information that can be exchanged and shared with other public authorities, partners and contractors in a secure environment.

Therefore, significant steps are being taken to identify the possible risks and determine the most robust and appropriate solutions. This report outlines proposed solutions and progress made in the twelve months proceeding the last report (30th April 2009) .

1.0 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.

2.0 Background Information

2.1 Leeds City Council has recognised the need to protect its information assets from both accidental and malicious loss or damage. Information security is taken very seriously by the Council and this is evidenced by the ongoing 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 ongoing to provide assurance on our approach to information security. In this regard it covers actions taken to address the policy framework and development, the skills and competencies required and the technology requirements within the organisation.

3.0 Main Issues

Framework and Policy Development

3.1 As Corporate Governance and Audit Committee are aware, Information Governance is part of the Council's Corporate Governance Framework, which was approved at Executive Board in November 2008. As part of an ongoing assessment, the Information Governance Framework is being reviewed in order to take account of external legislative and regulatory changes and internal strategy and policy requirements.

3.2 The Information Governance Framework covers the six broad areas of information governance including that pertaining to Information Security, Records Management and Data Quality. As part of the delivery of the Information Governance framework, an Information Security Policy was agreed and published and was reported to this Committee in January 2009. As part of this, work has continued during 2009/10 on policy development, and assessing the appropriate framework to use for information risk management.

3.3 The following policies and standards have been drafted and are in various stages of consultation throughout the Council:

- Removable Media Policy – establishing the principles and working practices to be adopted for information stored and transferred to all types of removable media;

- Leeds City Council Information Charter – as prescribed by the Information Commissioner, providing citizens with information about how the Council looks after their information;

- Protective Marking and Asset Control Policy – adopting a security classification scheme for all of the Council's information assets;

- Guidance to Managers on the use of Shared Drives – providing managers with advice about how to store sensitive personal information on the Council's network;

- Remote Working Policy – providing security and compliance guidance to the policy for aiding new and flexible ways of working for staff across the Council;

- Incident Management Policy – revising the current policy instructing staff on actions to be taken in cases whereby the Council's information security is compromised.

3.4 All of the above policies and standards once approved will be implemented and embedded across the Council during the course of 2010/11. These will be supported by further policy development during the next twelve months on Information Sharing; Information Risk Management; and, a Violent Warning Marker Policy. Furthermore the Council will be adopting a framework for assessing information risk and providing evidence-based assessment of performance. This framework is called the Information Assurance Maturity Model, which has been developed by the Cabinet Office for use across the public sector. This will be supported by the appointment of the Council's first Senior Information Risk Owner (SIRO).,The SIRO will have responsibility for information assurance risk management across the organisation and for providing assurances about information risk to the Chief Executive.

Skills and Competencies

3.5 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. Corporate Governance and Audit Committee will be aware from last year's report the intention to improve and strengthen the Council's capacity for implementing and maintaining information assurance across the organisation.

3.6 To this extent the Council appointed a Corporate Information Compliance Manager in October 2009 who has corporate and strategic responsibility for information assurance (Information Security and Information Sharing) and policy requirements for information compliance (Data Protection Act and Freedom of Information Act). This post is responsible for embedding best practice and for overseeing compliance with information security requirements across the Council.

3.7 In addition to corporate capacity, there is a requirement for a network of people across the organisation who will lead on embedding best practice across service areas and ensuring a coordinated approach to information security. Work is ongoing with Chief Officers for Resources and Support to identify suitable resources within the Directorates to provide capacity to implement and embed policy and practice and to monitor compliance of Information Assurance work.

3.8 Work continues to ensure the Council is able to share and receive information from other public organisations, partners and contractors through secure networks such as the Government Connect Secure Extranet (GCSx). Together with the delivery of the Information Governance Framework, implementation of this work will be monitored through strengthened governance arrangements and during 2010/11 the current Information Governance Group will be replaced by an Information Governance Management Board (IGMB). The IGMB will be supported by a number of sub-groups that will have responsibility for developing and embedding policy and practice for the specific information governance areas, one of which will have specific responsibility for information security and information sharing matters.

Technology

3.9 The Council was granted a connection to the Government Connect Secure Extranet (GCSx), a national network developed to permit secure data exchange between local authorities and central government departments, in September 2009. The network connection is now in daily use by staff within Leeds Benefits Service who access information held by The Department for Work and Pensions (DWP) during the processing of claims for Council Tax and Housing Benefit. The successful connection was the result of a long term commitment by the Council to improve the security of its network and information resources. This work is ongoing, as the connection was granted even though the Council has still not achieved full compliance with all of the security requirements outlined in the Government Connect (GC) Code of Connection (CoCo).

3.10 A decision was taken to engage a strategic partner in line with Corporate ICT Services policy of reducing the number of key suppliers and making strategic rather than tactical purchases. Following a tender exercise, McAfee was chosen as the provider of several key services, including network intrusion prevention; vulnerability management; endpoint security services; and, a secure web gateway.

3.11 The Endpoint Security services suite of products contains a software component that will prevent the unauthorized use of peripheral equipment such as memory sticks, CD's and DVD's and portable hard drives. Other notable procurements which have taken place include a system to manage the process of log file information from across the Council's ICT estate. This essentially provides the Council with a defence mechanism against unauthorized access to the system. The Council's network has also received several updates which support secure management of the network equipment, inline with best practice.

3.12 The deployment of these services has already begun, and is expected to be completed by autumn 2010.

4.0 Implications For Council Policy And Governance

4.1 The Information Governance Framework will be supported by the development of policies, procedures, guidance and best practice across the six modules of the Framework.

4.2 All Information Governance policies and procedures will follow a consultation process to obtain support and approval and this includes the Council's Information Governance Management Board and the Corporate Governance Board.

4.3 Corporate Governance and Audit Committee will receive an annual report on the implementation of information security across the Council and progress towards achieving adherence to national information assurance standards.

5.0 Legal And Resource Implications

5.1 The resource requirements for delivering the contents of the Information Governance Framework were outlined to Executive Board in November 2008, and provision has been made to meet these requirements in 2010/11.

5.2 Capacity within Directorates to deliver, embed and monitor compliance to information assurance policy and practice is required, but resources for this can be identified from existing FTE's within the Directorates.

5.3 There are no legal implications from this report.

6.0 Conclusions

6.1 Information Security has rightly been identified as a key area of risk and is being addressed through changes to policy, skills and technology. As this report demonstrates a number of initiatives are currently underway which will make a significant contribution to minimising the risks associated with poor information security.

7.0 Recommendations

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

Background Documents Used

The following documents were referenced to create this report:

- Annual Information Security Report to CG&A Committee 2009;
- Report to Corporate Governance Board on New Corporate Information Management Governance Arrangements – 4th February 2010;
- Report to Chief Officers Resources Strategy Group on Identifying Directorate Resources for Delivering Information and Knowledge Management Agenda and Changing the Workplace – 12th November 2009.