Report author: Andy Nutting & Jon Browne (ICT)

Tel: 07891 276168

Report of Assistant Chief Executive (Customer Access & Performance)

Report to Corporate Governance & Audit Committee

Date: 27th March 2012

Subject: Annual Information Security 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 outlines progress made in implementing and embedding the information governance policies across the Council and provides an assessment of each policy against the Council's Annual Governance Statement Standard.
2. 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.
3. The report details progress made by IT Services to implement a range of technologies to improve security across the Council.

Recommendations

4. 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

2.2 Leeds City Council recognises 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.

2.3 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 Main issues

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. This framework is underpinned by a number of key policies which enables the Council to meet its legal, regulatory, contractual and business obligations.

3.2 The development of these policies forms part of the Information Governance Project, which is ensuring all information governance policies are developed and a methodology for their effective communication, engagement and training across the Council put into place.

3.3 As part of this project, thirteen out of fourteen policies have been drafted, approved and signed-off for use across the Council. Each of the thirteen policies have been published on the Council's intranet site for access by staff and a series of key messages produced for reference by staff. Furthermore, a series of procedures and guidance notes are being produced to support the implementation of each policy. Most notably the Electronic Communications Code of Practice is currently with Trades Unions as part of the consultation process, but should be ready for publication and dissemination from April 2012 onwards. A Code of Practice on Social Media is in draft stage and will go out for consultation shortly. A procedure for investigating information security incidents will be approved after completing a final phase of consultation.

3.4 The fourteenth policy, on Information Risk Management is now being developed. This was purposefully delayed as it is reliant on the Council adopting an approach to information risk management as outlined in the Information Assurance strategy, which required approval and sign-off beforehand. The Information Assurance strategy was approved in October 2011 (see paragraphs 3.17 & 3.18), and as

such, a policy on Information Risk Management has now been drafted and is about to undertake a formal consultation process with key stakeholders.

3.5 An assessment of each policy has been undertaken based on the Council's Annual Governance Statement Standard to provide Members with the assurance they require about the arrangements being put in place to strengthen the security arrangements for the Council's information assets. The results of this assessment are produced in table format in Appendix One to this report.

3.6 The Information Commissioner's Office (ICO) has the power to fine organisations up to a maximum of £500,000 for a serious contravention of the Data Protection Act Principles. The Implementation and embedding of information assurance policies, standards and practice as outlined in this report is reducing the risk and helping to mitigate the Council against future information security incidents.

3.7 Whilst the implementation of information governance policies and procedures, and improved information practices, will do much to mitigate against the risk of information security incidents, it should be noted that this will not provide the Council with a guarantee of security breaches not happening in the future, and as such, we would be duty bound to report any major incident affecting personal data to the Information Commissioner.

Information Governance Policy Training

3.8 A training programme has been established to ensure all Council staff undertake training on the information governance policies. The training programme is a risk-based approach to learning and is delivering training on information governance in three phases.

3.9 Prior to the commencement of training, an information security checklist was issued to staff in October, which provided a 'Do's and Don'ts' on information practice and acts as an easy reference guide.

3.10 An audit of information risk across the Council has taken place identifying service areas that process sensitive information. An information matrix has been developed for each Directorate showing the correlation between the sensitivity of the information asset held and the quality of information practice in each service area. An example of this is attached at Appendix Three to this report. This information is being used to assess the level of information risk for each service area, which in turn is determining the training requirements for the service.

3.11 There are three levels of training in the training programme:

- Level One – E-Learning training for IT-Users and training brochure/leaflet for non-IT users;
- Level Two – Classroom based training and face-to face briefings to service areas identified as being a medium risk in managing information;
- Level Three – Targeted training for high risk service areas based on a gap analysis undertaken through information compliance audits.

3.12 **Level One Training**

All staff across the council have undertaken level one training between November 2011 and January 2012. This training encompassed the following:

- All IT-users undertaking training through an e-learning programme designed specifically to provide staff with key messages from all the information governance policies and requiring their sign-off for each policy to indicate that they have read and understood the information. This information is recorded onto the SAP system for monitoring purposes. This training took place between December 2011 and January 2012 ;

- Non-IT users who process sensitive information receiving information governance key messages via an Information Governance brochure and briefings by line managers. Manager's receiving brochures were instructed to ensure staff read and understood the information and report compliance to their appraisal coordinator. In turn, the appraisal coordinator recorded compliance onto the SAP system via the Business Support Centre. Brochures were distributed to managers in November 2011.

- Non-IT users who do not process sensitive information receiving leaflets providing key information about the policies. Leaflets were distributed in November 2011.

Training in Phase One is designed to make all staff aware of the information governance policies, understand the key messages, know where to locate each policy on the intranet for reference and where to go for further advice and guidance. Information recorded on the SAP system provides evidence that staff have undertaken the training should it be required for compliance purposes. Information about the performance of staff undertaking phase one training up to 9th March 2012 is provided Directorate by Directorate in the table below.

Directorate	Percentage return of staff undertaking training
Adult Social Care	86%
Children's Services	85%
City Development	85%
Environments & Neighbourhoods	82%
Legal Services	87%
Resources	95%
Customer Access & Performance	85%

3.13 The overall return across the Council is 87%. Whilst the figures are encouraging, further analysis work is being undertaken by Information Compliance Officers. This is to ensure that staff working in high risk areas complete the training. To this extent Information Compliance Officers are working with senior officers to identify these staff and ensure they complete the training. However, it should be noted that it will not be possible to achieve a 100% return across each Directorate, as some staff are away on either maternity leave, sick leave or long-term absence.

3.14 **Level Two Training**

Details about level two and three training are yet to be finalised, but it is likely that level two training will involve those service areas deemed as undertaking medium risk information management practices on the information matrix. These services will be required to undertake further training over and above that received at level one. An assessment will be made by Information Compliance Officer's and training tailored to specific needs developed and delivered either through face-to-face briefings or classroom based training.

3.15 **Level Three Training**

Level three training will involve those service areas identified as undertaking high risk information management practices on the information matrix and have a requirement to improve information management practice as well as undertake training. A self assessment information compliance audit will be used to identify weak information controls and potential risks with current information practices and provide recommendations for improved security arrangements and information procedures. The information compliance audit template has been

designed and is currently being piloted in the three area offices within Children's Services.

3.16 Information Governance messages have been embedded into the corporate induction checklist managers need to use with their new staff and staff changing roles. Human Resources reinforce this information at all their welcome events and in the staff guide that is given out at recruitment. The manager's checklist requires manager's to ensure new staff undertake the training on information governance as part of their induction.

Implementation of Information Assurance Strategy

3.17 A strategy for Information Assurance was approved in 2011. The aim of the strategy is to ensure that the Council meets its information management and security responsibilities ensuring that internal and external customers, partners and suppliers have the confidence that information, both personal and non-personal, is handled and stored with due regard to its value and risk, where individuals understand the importance of using it correctly, sharing it lawfully and protecting it from improper use.

3.18 To support both the Information Governance Framework and the implementation of the Information Assurance strategy, work is ongoing to improve and strengthen information risk management and information security across the council. This ongoing work is highlighted in the table at Appendix Two to this report and provides further assurance in respect of the continued work being undertaken to provide security to the council's information assets.

Skills and Competencies

3.19 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.

3.20 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 are undertaking a review of resource requirements to ensure that there is adequate information governance capacity across the Directorate. Discussions are ongoing with the Strategic Landlord about providing a resource in the new ALMO's Business Centre Limited to implement information governance requirements across the three ALMO's.

3.21 Whilst there is an information governance resource within each Directorate, arrangements vary within each Directorate and it is difficult to provide assurance about the consistency to the delivery and implementation of the Information Governance Framework across the Council. A review of Information Governance resource requirements is being undertaken through the Information and Content Management project, to look at ways of implementing information governance standards and practice in a more professional and cost effective manner.

3.22 Governance arrangements for information governance across the Council are now firmly embedded. The Information Governance Management Board meets every two months and is responsible for overseeing the delivery of the Information Governance Framework. The Information Governance Management Board is supported in this work by four sub-groups, each responsible for delivering particular aspects of the Information Governance Framework. Both the Information Governance Management Board and four Sub-Groups were established in 2010 and provide a governance framework for ensuring the delivery of information governance and monitoring compliance to associated policies, procedures and practice. Furthermore, the Assistant Chief Executive (Customer Access and Performance) acts in the capacity of the Council's Senior Information Risk Owner.(SIRO). The SIRO is ultimately accountable for the assurance of information security at the Council. The Local Government Association has said that all local authorities should designate a board member as SIRO..

Technology

3.23 Significant progress has been made over the last eighteen months to implement a range of technologies to improve security across the Council. The progress made in commissioning and installing the technologies has enabled IT to report statistics which it was unable to report prior to the deployment.

3.24 ICT Services are now able to enforce the policy on USB devices which will limit their use within the council. Only council approved encrypted USB devices will be able to have information written to them. All other devices will be rendered as read only devices unless they have submitted a request under the Policy Exemption procedure. This will still enable users to review their camera pictures etc., but will disable their ability to use non council USB devise as data stores.

3.23 McAfee Vulnerability Manager has now been commissioned and is scanning all network attached devices, from which IT Services can see what versions of software are being used across the estate. Once this information is collated IT Services can develop a schedule of approved versions which can then be applied consistently across the network.

3.24 The LogRhythm Security Information and Event Management (SIEM) device is now monitoring critical components within the network. It is monitoring failed logon attempts, unauthorised changes to configurations and critical file monitoring and provides an administrative dashboard which records and shows critical events such as unusual or unauthorised activity or file compromise. This is being expanded to cover more systems, and all critical events are being investigated. A part of the LogRhythm implementation is the deployment of File Integrity Management (FIM) which watches for changes being made on critical files within an application. This has been deployed on the Payment Card Industry-Data Security Standard environment (see below).

Critical Services, such as the Payment Card Industry-Data Security Standard Merchant payment system used for council tax collection, are heavily monitored. Indeed, during a recent maintenance session Northgate, the software vendor of the payment system, modified one of the protected files without informing the security team. The monitoring system logged the change and instantly generated a security alert which triggered the Incident Management procedure. This identified that the file

had been tampered with and Northgate then confirmed that it was they that had modified the file.

In respect of third parties and contractors, all access to council resources is risk assessed prior to granting access to Council information systems. Data Handling agreements are put in place and there are strict access procedures to which contractors and third party support companies must adhere. No access is granted directly to devices, rather all access is granted via an intermediate service, or proxy, through the use of terminal service session controlled by Citrix. Access is limited to the relevant server or services only. Access is controlled by IT services and must use two factor authentication through the use of a once time use code generating token. The token is held by IT Services which ensures that they are notified of any access being granted.

3.25 The McAfee Web Gateway Internet filter has now replaced the Novell Border Manager and is providing active content filtering and policy enforcement, including the blocking of executable file downloads, and content type mismatches. It is also providing users with some feedback as to the reason a site has been blocked. ICT Services are now able to provide some statistics on web use

3.26 Leeds City Council ICT Services runs the Microsoft Exchange based email system under the terms of the Acceptable Use policy. System administrators by default have no access to email boxes, however ICT Services are the custodian of all the council IT systems and as such retain the right to escalate privileges to allow access to all system data to a select few. Systems administrators take their duties seriously and understand the confidential nature of Members correspondence.

3.27 There are instances, however, where some emails, both inbound and outbound, are quarantined by the system as being suspected SPAM messages or messages containing viruses or blocked attachments. Currently these have to be interrogated manually prior to deletion or release to the end user. A few email specialist support staff are authorised to perform this function and other related functions such as mail box and message recovery. These actions are considered a necessity for the smooth running of this large, complex and mission critical council system.

3.28 IT Services is investigating the possibility of a self service release system where each email user will be sent an email (spam digest) with a list of the messages blocked by the system. They will then be able to select those that are genuine messages (false positives) and release them to their own inbox. In the meantime this process is performed manually.

3.29 Members email is retained post their retirement and made available to them for a period of 30 days after leaving office. Offline stores may be made available to the Member subject to a security review. Backups of Member email are held for 6 months and then deleted.

4. Corporate Considerations

Consultation and Engagement

4.1 Consultation on the development of all information governance policies has been extensive and 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 Pilots have been undertaken on new practice and procedures, for example on Government Protective Marking Scheme and Information Compliance Audits, in order to fully test out requirements and obtain feedback and engagement from those involved and introduce improvements to processes as a result.

Equality and Diversity / Cohesion and Integration

4.3 All policies have been developed as part of the Information Governance Project which has developed a training programme for all staff and partners with respect to information governance. Equality, diversity, cohesion and integration are all being considered as part of this programme of work. This refers to the way in which the training is being delivered as well as how the policies will impact on staff and partners.

Council policies and City Priorities

4.4 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.

4.5 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.

Resources and value for money

4.6 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.

Legal Implications, Access to Information and Call In

4.7 There are no legal implications from this report.

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

Risk Management

4.8 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 it's citizens, partners, contractors and third parties when handling and storing sensitive and protectively marked information.

4.9 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 it's IT network infrastructure and exposes information assets to unnecessary security risks.

5. Conclusions

5.1 Information Security has rightly been identified as a key area of risk and is being addressed through changes to policy, procedure and practice, training, and technology. As this report demonstrates a range of policies on information governance have been developed, and new technologies procured to reduce the risk to the Council's information assets. However there is a still much to do, and therefore the focus over the next twelve months will be to continue the training and embedding the policies across the Council through a risk management approach. 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

7.1 Information Governance Framework and associated policies

7.2 Information Governance – Learning and Training Strategy

7.3 CRAIG Framework – Business Case for creating SIRO role

7.4 GPMS Requirements Business Case

7.5 Information Incident Management Policy

7.6 Information Sharing Policy

Information Governance Project Appendix One

Information Governance Policy Assessment based on Annual Governance Statement Standard

Name of Policy	How up to date is the policy?	Is the policy fit for purpose?	How has the policy been communicated across the organisation?	Is the policy routinely complied with?	How is the policy monitored?
Information Security	Current	Yes (reviewed 2011)	Previous version published on intranet. New policy key messages have been communicated through corporate training programme developed by the Information Governance Project. IT Users have undertaken e-learning training programme between Dec 2011 and Jan 2012 and non-IT users received a training brochure or leaflet. A link to the full policy is provided which is published on the intranet. User compliance to training monitored via the BSC using the SAP system. Further training to be developed as part of a phased IG training programme for those users determined as high risk and medium risk operators. There will be specific training for Information Asset Owner's and users with specific Information Assurance responsibilities as well as training for users working in joint teams with different organisational policies & procedures	Policy compliance will be measured using data returns on e-learning tests and non-IT training, staff perception surveys and improved scores on compliance frameworks such as the Information Assurance Maturity Model and internal audit on Data Handling Guidelines Directorate Information Compliance Officers, with the support of Local Information Officer's will ensure the policy requirements are implemented effectively. Information Compliance Audit is being piloted in Children's Services. These will be used in high risk service areas to identify weak information practice and procedures, as well as monitor compliance with policy.	Compliance with the policy, together with the policy's effectiveness, demonstrated by the nature, number and impact of recorded information security incidences, will be reviewed in line with the corporate information audit to be undertaken every three years by the Information Governance Team and Directorate Information Governance resources, and interim information audits across the Council. The policy will be reviewed by the corporate Information Governance Team, or as appropriate and in response to changes to legislation or council policies, technology, increased risks & new vulnerabilities or in response to security incidents.

			Forms part of Terms & Condition's in contracts.		
Records Management	Current	Yes (reviewed 2011)	Previous version published on intranet. New policy key messages have been communicated through corporate training programme developed by the Information Governance Project. IT Users have undertaken e-learning training programme between Dec 2011 and Jan 2012 and non-IT users received a training brochure or leaflet. A link to the full policy is provided which is published on the intranet. User compliance to training monitored via the BSC using the SAP system. Further training to be developed as part of a phased Information Governance training programme for those users determined as high risk and medium risk operators. Further awareness training already conducted by Directorate Records Manager's preparing paper records for transfer to Facility.	Policy compliance will be measured using data returns on e-learning tests and non-IT training, staff perception surveys and improved scores on compliance frameworks such as the Information Assurance Maturity Model and internal audit on Data Handling Guidelines. Directorate Records Manager's with the support of Local Information Officer's will ensure records standards are maintained across each Service Area. Information Compliance Audit is being piloted in Children's Services. These will be used in high risk service areas to identify weak information practice and procedures, as well as monitor compliance with policy.	The policy will be reviewed by the corporate Information Governance Team, or as appropriate and in response to changes to legislation or council policies, technology, increased risks & new vulnerabilities or in response to security incidents.
Information Sharing	Current	Yes	Policy published on the intranet. Key messages have been communicated as part of the corporate training programme. IT Users have undertaken e-learning training programme between Dec 2011 and Jan 2012 and non-IT users received a training brochure	Policy compliance will be measured using data returns on e-learning tests and non-IT training, staff perception surveys and improved scores on compliance frameworks such as the Information Assurance Maturity Model and internal audit	The policy will be reviewed by the corporate Information Governance Team, or as appropriate and in response to changes to legislation or council policies, technology, increased risks and new vulnerabilities or in response to security incidents.

			or leaflet. A link to the full policy is provided which is published on the intranet. User compliance to training monitored via the BSC using the SAP system. Further training to be developed as part of a phased Information Governance training programme for those users determined as high risk and medium risk operators. Some areas of the Council already have an awareness of the information sharing requirements through the use of the Inter-agency Information Sharing Protocol. Forms part of Terms & Condition's in contracts.	on Data Handling Guidelines Directorate Information Compliance Officers , with the support of Local Information Officer's will ensure the policy requirements are implemented effectively. Information Compliance Audit is being piloted in Children's Services. These will be used in high risk service areas to identify weak information practice and procedures, as well as monitor compliance with policy.	Where practical and proportional, Corporate ICT Services will monitor users' access to information for the purpose of detecting breaches of this policy and/or other council policies and procedures. A register of information sharing documentation will be maintained corporately to ensure compliance with the policy and consistency across the council.
Information Risk Management	To be developed in line with the proposed Information Assurance strategy.	Required approval of the Information Assurance Strategy before possible to start this policy. Approval for strategy obtained in November 2011. Report in draft format.	N/A	N/A	N/A
Information Security Incident Management Reporting	Current	Yes	Policy published on the intranet. Key messages have been communicated as part of the corporate training programme. IT Users have undertaken e-learning	Policy compliance will be measured using data returns on e-learning tests and non-IT training, staff perception surveys and improved scores on	The policy will be reviewed by the corporate Information Governance Team, or as appropriate and in response to changes to legislation or council

			training programme between Dec 2011 and Jan 2012 and non-IT users received a training brochure or leaflet. A link to the full policy is provided which is published on the intranet. User compliance to training monitored via the BSC using the SAP system. Some awareness training already undertaken with Information Compliance Officers – aligns with policy exemption process. Classroom based training rolled out to approx 550 staff undertaking new ways of working though Changing the Workplace	compliance frameworks such as the Information Assurance Maturity Model and internal audit on Data Handling Guidelines. The corporate Information Governance Team will monitor the number of incidents by reviewing reports on the Council's Remedy System. To be linked to the new procedure for Information Investigation and Directorate Information Compliance Officers, with the support of Local Information Officer's will ensure the policy requirements are implemented effectively.	policies, technology, increased risks and new vulnerabilities or in response to security incidents. Where practical and proportional, Corporate ICT Services will monitor users' access to information for the purpose of detecting breaches of this policy and/or other council policies and procedures. Compliance with the policy, together with the policy's effectiveness, demonstrated by the nature, number and impact of recorded information security incidences, will be reviewed in line with the corporate information audit to be undertaken every three years by the Information Governance Team and Directorate Information Governance resources, and interim information audits across the Council.
Protective Marking & Asset Control	Current	Yes	Policy published on the intranet. Whilst key messages have been communicated as part of the corporate training programme, specific training on Government Protective Marking Scheme will be provided as and when process is rolled out. Staff guidance has been drafted in support of the policy. Awareness training undertaken as part of the corporate Information Governance training programme	Policy compliance will be measured using data returns on e-learning tests and non-IT training, staff perception surveys and improved scores on compliance frameworks such as the Information Assurance Maturity Model and internal audit on Data Handling Guidelines. Directorate Information Compliance Officers, with the support of Local Information	The policy will be reviewed by the corporate Information Governance Team, or as appropriate and in response to changes to legislation or council policies, technology, increased risks and new vulnerabilities or in response to security incidents. Where practical and proportional, Corporate ICT Services will monitor users' access to information for the purpose of

			between Dec 2011 & Jan 2012.. Pilots are being carried out in Peace & Emergency Planning Unit, Children's Safeguarding Board and Community Safety prior to roll-out across the council.	Officer's will ensure the policy requirements are implemented effectively.	detecting breaches of this policy and/or other council policies and procedures.
Information Systems Acceptable Use	Current	Yes	Policy published on the intranet. Key messages have been communicated as part of the corporate training programme. IT Users have undertaken e-learning training programme between Dec 2011 and Jan 2012 and non-IT users received a training brochure or leaflet. A link to the full policy is provided which is published on the intranet. User compliance to training monitored via the BSC using the SAP system. Further training to be developed as part of a phased Information Governance training programme for those users determined as high risk and medium risk operators. Classroom based training rolled out to approx 550 staff undertaking new ways of working though Changing the Workplace. There are a number of supporting documents to this policy which are still being developed e.g. Electronic Communications Code of Practice, Social Media Code of Practice, Password Guidance & Monitoring Policy.	Policy compliance will be measured using data returns on e-learning tests and non-IT training, staff perception surveys and improved scores on compliance frameworks such as the Information Assurance Maturity Model and internal audit on Data Handling Guidelines. Directorate Information Compliance Officers, with the support of Local Information Officer's will ensure the policy requirements are implemented effectively. Information Compliance Audit is being piloted in Children's Services. These will be used in high risk service areas to identify weak information practice and procedures, as well as monitor compliance with policy.	The policy will be reviewed by the corporate Information Governance Team, or as appropriate and in response to changes to legislation or council policies, technology, increased risks and new vulnerabilities or in response to security incidents. Where practical and proportional, Corporate ICT Services will monitor users' access to information for the purpose of detecting breaches of this policy and/or other council policies and procedures. Compliance with the policy, together with the policy's effectiveness, demonstrated by the nature, number and impact of recorded information security incidences, will be reviewed in line with the corporate information audit to be undertaken every three years by the Information Governance Team and Directorate IG resources, and interim information audits across the Council.

Data Protection	Current	Yes (reviewed 2011)	Previous version published on intranet. New policy key messages have been communicated through corporate training programme developed by the Information Governance Project. IT Users have undertaken e-learning training programme between Dec 2011 and Jan 2012 and non-IT users received a training brochure or leaflet. A link to the full policy is provided which is published on the intranet. User compliance to training monitored via the BSC using the SAP system. Further training to be developed as part of a phased Information Governance training programme for those users determined as high risk and medium risk operators. Classroom based training rolled out to approx 550 staff undertaking new ways of working though Changing the Workplace	Policy compliance will be measured using data returns on e-learning tests and non-IT training, staff perception surveys and improved scores on compliance frameworks such as the Information Assurance Maturity Model and internal audit on Data Handling Guidelines. Data Protection Practitioner's monitor and will continue to monitor compliance to the Data Protection Act within their respective Directorates. Information Compliance Audit is being piloted in Children's Services. These will be used in high risk service areas to identify weak information practice and procedures, as well as monitor compliance with policy.	The policy will be reviewed by the corporate Information Governance Team, or as appropriate and in response to changes to legislation or council policies, technology, increased risks and new vulnerabilities or in response to security incidents. The Council's Data Protection Practitioner's will be engaged in the review to ensure processes and procedures are reviewed as part of the annual review. Where practical and proportional, Corporate ICT Services will monitor users' access to information for the purpose of detecting breaches of this policy and/or other council policies and procedures.
Freedom of Information/Environmental Information Regulations	Current	Yes	Policy published on the intranet. Key messages have been communicated as part of the corporate training programme. IT Users have undertaken e-learning training programme between Dec 2011 and Jan 2012 and non-IT users received a training brochure or leaflet. A link to the full policy is provided which is published on the intranet. User compliance to training monitored via the BSC using the SAP system.	Policy compliance will be measured using data returns on e-learning tests and non-IT training, staff perception surveys and improved scores on compliance frameworks such as the Information Assurance Maturity Model and internal audit on Data Handling Guidelines. Data Protection Practitioner's monitor and will continue to monitor compliance to the	The policy will be reviewed by the corporate Information Governance Team, or as appropriate and in response to changes to legislation or council policies, technology, increased risks and new vulnerabilities or in response to security incidents. The Council's Data Protection Practitioner's will be engaged in the review to ensure processes and procedures are reviewed as

				Freedom of Information Act and Environmental Regulations within their respective Directorates. Information Compliance Audit is being piloted in Children's Services. These will be used in high risk service areas to identify weak information practice and procedures, as well as monitor compliance with policy.	part of the annual review. Where practical and proportional, Corporate ICT Services will monitor users' access to information for the purpose of detecting breaches of this policy and/or other council policies and procedures.
Remote Access	Policy approved by Information Governance Management Board on 15th Sept.	Yes	Policy will be published on the intranet and key messages have been communicated as part of the corporate training programme. IT Users have undertaken e-learning training programme between Dec 2011 and Jan 2012 and non-IT users received a training brochure or leaflet. A link to the full policy is provided which is published on the intranet. User compliance to training monitored via the BSC using the SAP system. Further training to be developed as part of a phased IG training programme for those users determined as high risk and medium risk operators.	Policy compliance will be measured using data returns on e-learning tests and non-IT training, staff perception surveys and improved scores on compliance frameworks such as the Information Assurance Maturity Model and internal audit on Data Handling Guidelines. Information Compliance Audit is being piloted in Children's Services. These will be used in high risk service areas to identify weak information practice and procedures, as well as monitor compliance with policy.	The policy will be reviewed annually by IT Security Team, or as appropriate and in response to changes to legislation or council policies, technology, increased risks and new vulnerabilities or in response to security incidents. Where practical and proportional, Corporate ICT Services will monitor users' access to information for the purpose of detecting breaches of this policy and/or other council policies and procedures.
Clear Desk/Clear Screen	Current	Yes	Policy published on the intranet. Key messages have been communicated as part of the corporate training programme. IT Users have undertaken e-learning training programme between Dec	Policy compliance will be measured using data returns on e-learning tests and non-IT training, staff perception surveys and improved scores on compliance frameworks such as	The policy will be reviewed by the corporate Information Governance Team, or as appropriate and in response to changes to legislation or council policies, technology, increased

			2011 and Jan 2012 and non-IT users received a training brochure or leaflet. A link to the full policy is provided which is published on the intranet. User compliance to training monitored via the BSC using the SAP system. Further training to be developed as part of a phased Information Governance training programme for those users determined as high risk and medium risk operators. Classroom based training rolled out to approx 550 staff undertaking new ways of working though Changing the Workplace	the Information Assurance Maturity Model and internal audit on Data Handling Guidelines. Directorate Information Compliance Officers, with the support of Local Information Officer's will ensure the policy requirements are implemented effectively. Information Compliance Audit is being piloted in Children's Services. These will be used in high risk service areas to identify weak information practice and procedures, as well as monitor compliance with policy.	risks and new vulnerabilities or in response to security incidents. Where practical and proportional, Corporate ICT Services will monitor users' access to information for the purpose of detecting breaches of this policy and/or other council policies and procedures.
Removable Media and Mobile Computing	Current	Yes	Policy published on the intranet. Key messages have been communicated as part of the corporate training programme. IT Users have undertaken e-learning training programme between Dec 2011 and Jan 2012 and non-IT users received a training brochure or leaflet. A link to the full policy is provided which is published on the intranet. User compliance to training monitored via the BSC using the SAP system. Further training to be developed as part of a phased IG training programme for those users determined as high risk and medium risk operators. Further training to be developed as part of a phased Information Governance training programme	Policy compliance will be measured using data returns on e-learning tests and non-IT training, staff perception surveys and improved scores on compliance frameworks such as the Information Assurance Maturity Model and internal audit on Data Handling Guidelines. Directorate Information Compliance Officers, with the support of Local Information Officer's will ensure the policy requirements are implemented effectively. Information Compliance Audit is being piloted in Children's Services. These will be used in high risk service areas to identify weak information practice and	The policy will be reviewed by the corporate Information Governance Team, or as appropriate and in response to changes to legislation or council policies, technology, increased risks and new vulnerabilities or in response to security incidents. Where practical and proportional, Corporate ICT Services will monitor users' access to information for the purpose of detecting breaches of this policy and/or other council policies and procedures.

			for those users determined as high risk and medium risk operators. Classroom based training rolled out to approx 550 staff undertaking new ways of working though Changing the Workplace	procedures, as well as monitor compliance with policy.	
Record Retention & Disposal	Current	Yes	Policy published on the intranet. Key messages have been communicated as part of the corporate training programme. IT Users have undertaken e-learning training programme between Dec 2011 and Jan 2012 and non-IT users received a training brochure or leaflet. A link to the full policy is provided which is published on the intranet. User compliance to training monitored via the BSC using the SAP system. Further training to be developed as part of a phased IG training programme for those users determined as high risk and medium risk operators.	Policy compliance will be measured using data returns on e-learning tests and non-IT training, staff perception surveys and improved scores on compliance frameworks such as the Information Assurance Maturity Model and internal audit on Data Handling Guidelines. A corporate retention schedule is being developed and Directorate Records Manager's are responsible for implementing and monitoring effective use of retention periods on their service records.	The policy will be reviewed by the corporate Information Governance Team, or as appropriate and in response to changes to legislation or council policies, technology, increased risks and new vulnerabilities or in response to security incidents. Where practical and proportional, Corporate ICT Services will monitor users' access to information for the purpose of detecting breaches of this policy and/or other council policies and procedures.
Information & Data Quality			Policy published on the intranet. Key messages have been communicated as part of the corporate training programme. IT Users have undertaken e-learning training programme between Dec 2011 and Jan 2012 and non-IT users received a training brochure or leaflet. A link to the full policy is provided which is published on	Policy compliance will be measured using data returns on e-learning tests and non-IT training, staff perception surveys and improved scores on compliance frameworks to be adopted such as the Information Assurance Maturity Model and internal audit on Data Handling Guidelines.	The policy will be reviewed by the corporate Information Governance Team, or as appropriate and in response to changes to legislation or council policies, technology, increased risks and new vulnerabilities or in response to security incidents. Where practical and proportional,

			the intranet. User compliance to training monitored via the BSC using the SAP system. Further training to be developed as part of a phased IG training programme for those users determined as high risk and medium risk operators.	A Data Quality Working Group comprising of DQ Officers from each Directorate will monitor compliance with policy principles.	Corporate ICT Services will monitor users' access to information for the purpose of detecting breaches of this policy and/or other council policies and procedures.
Policy Exemption Process	Current	Yes	Exemption process workshop undertaken with Information Compliance Officers. It is for Information Compliance Officer's and Local Information Officer's to identify risks and assess whether an exemption is required.	Policy compliance will be measured by maintaining a record of the number of exemptions in existence and the regular review of each exemption. Consideration will be given to how well the process is working across the organisation.	The process will be reviewed by the corporate Information Governance Team, or as appropriate and in response to internal change requirements ordained by making the process more effective for users.

Appendix Two

Information Assurance Work Programme

Information Assurance Work	Work Progress to Date	Work Requirements	Assurance Required
Senior Information Risk Owner	Appointment of Assistant Chief Executive (Customer Access & Performance) 8th Feb 2011	Senior Information Risk Owner to undertake national training requirements Apr – Jun 2012	Local Government Association guidance and other best practice recommend all public authorities appoint a senior officer at board level as Senior Information Risk Owner. Senior Information Risk Owner is ultimately accountable for the assurance of information security within the council.
Information Asset Register and Appointment of Information Asset Owners	Information Asset Register completed. . Information Asset Owner assigned to each Information Asset.	Training to of all Information Asset Owners to take place 2012/13 to ensure responsibilities are understood. Ongoing monitoring of Information Asset Register to take place.	Information Asset Register provides council with details about all information assets held and accountability for those assets. Local Government Association guidance recommends councils appoint senior managers as Information Asset Owner's to be accountable for main information systems and information assets
Implementation of security classification adopting the Government Protective Marking Scheme	Protective Marking and Asset Control policy approved. Staff guidance produced. Pilot of manual implementation of Government Protective Marking Scheme underway within 3 service areas across the council - Dec 2011/ May 2012.	Staff guidance to be approved and published. Analysis report of the pilots to be drafted and published. Market testing of Government Protective Marking Scheme software solution to be undertaken – Mar/Apr 2012. Business case of options to implement Government Protective Marking	Requirement to ensure the right balance is struck between sharing and protecting information, therefore the business impacts and risks associated with the confidentiality, integrity and availability of information must be managed effectively. A primary building block in developing effective and appropriate security measures is to identify those information assets which need safeguarding. The Government Protective

		Scheme enterprise wide to be drafted as part of Electronic Document & Records Management System project Apr – Jun 2012	Marking Scheme (Government Protective Marking Scheme) is an information security classification system that achieves this. It is already widely used across central government and other local authorities.
Development of Information Incident Management and Investigation Procedure	Information Incident Management policy approved. IT System (Remedy) for recording information incidents being developed for use. Information Security Investigations procedure drafted and being consulted on.	Sign-off development work on Remedy system. Train Information Compliance Officer's on Remedy system and incident and investigation procedure. Centrally record all information security incidents and issue remedial reports	Requirement to ensure the council has a process for tracking, recording and responding to information security incidents. It requires a procedure for investigating, reporting and learning from such incidents, and a process for corporately recording and analysing data about incidents.
Strengthen Information Sharing arrangements across the council	Information Sharing policy approved and signed off. Included in standard T's & C's for contracts. Council signed up to updated West Yorkshire Information Sharing Protocol. Information sharing and security checklist produced for Contract and Commissioning Teams. Workshop undertaken with Children's Services Contract & Commissioning Team and Information Governance to be incorporated into work undertaken by this team.	Information Compliance Officer's to provide advice and guidance about information sharing agreements, data processing agreements & non-disclosure agreements. Organise workshops with all Contract & Commissioning staff and promote Information Governance checklist. Ensure Privacy Impact Assessments become part of the council's project implementation process.	Increasing requirement to share council information with partners, contractors and 3rd parties. In order to ensure the most effective service delivery and the council meets it's legal obligations relevant information has to be shared efficiently and securely.
Delivery of secure email to high risk service areas	Roll out of GCSx Secure Email accounts to high risk service areas.	Options paper to be considered by IGMB – March 2012 Development of a strategy for the	As part of the Government Connect and other secure network programmes there is a requirement to transfer and receive

		implementation of a secure email infrastructure in high risk service areas across the Council – Apr – Jun 2012	data in a safe and secure way. The Council is required to be able to exchange Protectively Marked information over a secure email GCSx network.
Develop Information Risk Management Policy to support the approved IA Strategy	Draft policy developed in line with corporate risk management methodology.	Policy to undertake full consultation process. Approval of policy at future IGMB. Sign-off and publication of policy Communication and training rollout of policy.	The council has approved the introduction and embedding of information risk management into its business functions through the Information Assurance Strategy. Information risk is inherent in all functions undertaken by the council. It is widely accepted that the aim of information risk is not to eliminate risk, but rather to provide a structural means to identify, prioritise and manage these risks.
Undertake a review of all information governance policies, ensuring changes to legislation, regulations and standards are implemented, in addition to amendments to internal practice and procedure. Rationalise and amalgamate some of the Information Governance policies as the organisation reaches a level of information governance maturity acceptable to do this.	All policies are amended to reflect changes to legislation, regulations, standards and internal practice and procedure. All policies are subject to a complete review every three years.	Key stakeholders are involved in the review of Information Governance policies through an established consultation process.	All Information Governance policies reflect requirements to protect the Council's information assets, and are subject to review to accommodate any necessary changes, both from a national and internal perspective.

Example of the Information Matrix referred to in the report at paragraph 3.7 Appendix Three

Customer Access & Performance

SENSITIVITY OF INFORMATION	Low	Medium	High
High	International Relations - Staff Reports Management & Support - Draft Policy Management & Support Staff Records Policy & Performance Staff Records Policy & Performance Draft Policy Leeds Initiative - Staff Records Leeds initiative - Draft Policy Equality - Staff Records Regional Policy - Staff Records Admin Support 3	Customer Services- Systems Support Team 6	Customer Services- Customer Data 9
Medium	2	Equality - Personal Contact Details Regional Policy - Personal Contact Details Leeds Initiative - Personal Contact Details Policy & Performance - Personal Contact Details Management & Support - Personal Contact Details International relations - Personal Contact Details 4	6
Low	Equality - Data Records Equality - Accounting /Budget records Regional Policy - Accounting /Budget records Leeds Initiative - Accounting & Budget records Policy & Performance Accounting / Budget records Policy & Performance - Corporate Performance Reports Management & Suppport - Accounting & Budget records International Relations - Accounting & Budget Records 1	2	3

Risk