Leeds
CITY COUNCIL

Originator: Andrew Nutting

Tel: 07891 276168

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

Corporate Governance and Audit Committee

Date: 21st March 2011

Subject: Annual Information Security Report

Electoral Wards Affected:

□ Ward Members consulted (referred to in report)

Specific Implications For:

Equality and Diversity □

Community Cohesion □

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 report provides Members with information about the progress of policies being developed as part of the Information Governance project and the intention to consult the implications of these policies for Members through the Members Development Working Group. The delivery of these policies will strengthen security arrangements for the Council's information assets. Appendix A to the report provides Members of this Committee with information being provided to the Members Development Working Group and an opportunity to comment.

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 (17th March 2010) .

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 In April 2010 the Information Commissioner's Office (ICO) was granted new powers to fine organisations up to a maximum of £500,000 for breaches of the Data Protection principles. These new powers were used on 24th November 2010 when the ICO fined Hertfordshire County Council £100,000 for two incidents whereby an employee faxed sensitive personal information to the wrong recipients. A second monetary penalty of £60,000 was issued to employment services company A4e for the loss of an unencrypted laptop containing personal information of up to 24,000 clients. Further to this the ICO issued a second wave of fines on 8th February 2011. The London Boroughs of Ealing and Hounslow were fined £80,000 and £70,000 respectively for breaches to the Data Protection Act. In the case of both councils, an out-of-hours service that works on behalf of both councils lost two laptops containing the details of around 1,700 individuals when they were stolen from an employee's home. Whilst the laptops were password protected, they were unencrypted in breach of both council's policies. The ICO ruled that Ealing Council breached the Data Protection Act by issuing an unencrypted laptop to a member of staff in breach of its own policies. It said that Hounslow Council breached the act by failing to have a written contract in place with Ealing Council. Hounslow also did not monitor Ealing Council's procedures for operating the service securely. The ICO has indicated an intent to use these powers on other organisations that breach the Data Protection Act. The implementation of information governance policies and other work ongoing and outlined in this report will help to protect the Council and mitigate against potential breaches of the Data Protection Act.

3.2 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. The review will be completed and consultation and sign-off of the Information Governance Framework undertaken at the Information Governance Management Board in March 2011.

3.3 The Information Governance Framework covers the six broad areas of information governance including that pertaining to Information Security, Records Management, Information Sharing 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. This policy is being reviewed as part of the Information Governance project. More recently policies on Remote Working, Removable Media and Mobile Computing, Protective Marking and Asset Control, and Clear Desk and Clear Screen have received sign-off. These will be further supported with additional policies, procedures, guidance and standards currently being developed, including:

- Information Incident Management Policy
- Information Sharing Policy;
- Information Systems Acceptable Use Policy;
- Records Management;
- Records Retention & Disposal Policy
- Data Protection
- Freedom of Information & Environmental Information Regulations Policy; and
- Information Risk Management Policy
- Remote Access Policy

3.4 The development of these policies forms part of the Information Governance Project. The aim of the Information Governance project is to ensure all Information Governance policies are developed and to provide a methodology for the effective communications, engagement and training of these policies across the Council. ICT Services are contributing to the development of these policies in order to ensure they support the implementation of security systems and related technologies.

3.5 As a result of the increased powers of the Information Commissioner, the Council determined a need to have these policies in place as quickly as possible, in order to minimize the risk of financial penalties being imposed on it and the subsequent reputational damage this would cause. These policies are to be deployed and embedded through a number of Council programmes such as Changing the Workplace and are therefore subject to tight times schedules.

3.6 The Information Governance project recognises the importance of engagement with Members and discussions are under way on how best to facilitate this process. Some consultation about the implication of these policies on Members has already been facilitated through the Members Development Working Group via the Members Development officer, and in particular, the best way of delivering key messages. Further consultation is planned with Members during 2011/12 around how the implications of the policies will impact on Members themselves. The way policies are implemented will be managed through a risk management process. A policy exemption process is being developed to allow specific business requirements to be assessed against policy should this be deemed necessary. Appendix A provides details of each policy, including an overview of each policy and possible implications for Members as each policy stands.

3.7 Each policy is subject to an annual review to ensure that they are updated to reflect changes to legislation, technology, increased risk and new vulnerabilities or changes to Council policy. As part of the review each policy will undertake a brief consultation with key stakeholders to ensure they are fit for purpose and the process will be monitored by the Information Governance Management Board.

3.8 There are three delivery mechanisms for ensuring effective communication of the policies. These include:

- Changing the Workplace – policies are communicated as part of a structure change and work package, which will involve managers workshops, and presentations and briefings to staff;

- Electronic Document and Records Management (EDRMS) – policies that compliment the implementation of the EDRMS will be communicated and trained out to staff during the roll out and deployment of the technology and change processes as and when each service deploys this technology; and,

- Deployment through Information Governance specialist staff – a face-to-face and an e-learning package informing employees of the practical application and key messages of the policies is available to be deployed by Information Governance specialist staff (Records Managers, Information Compliance Officers) across each Directorate.

Furthermore, discussions with HR will take place about integrating information governance and policy learning requirements into staff appraisals and staff induction programmes.

Policies relating to the compliance of the Council's information assets will be monitored by ICT services as detailed in section 3.18 of this report. Additionally, ICT will be tracking the return of ICT equipment and Finance will be monitoring ICT spending to ensure that only corporate ICT approved equipment is purchased. In respect of the Changing the Workplace programme, managers will be trained on information governance awareness to ensure that staff receive training appropriate to their needs. Once new ways of working are in place, because managers have been trained and made aware of Information Governance, they are able to monitor employees behaviour in relation to the practical application of the policies. In respect of the EDRMS, key aspects of related policies will be built into the systems and automated. However, there will be elements that require input by staff and the communications of these will be delivered with the deployment of the technology. In respect of the policies relating to access to information legislation such as the Data Protection Act, these will be trained as part of the processes outlined above, and compliance will be monitored in respect of the number of complaints made by members of the public.

Further details of the training and communications intended to deploy and embed Information Governance can be provided per policy on request.

3.9 During 2010/11, work has been ongoing to develop the Council's first Information Asset Register. The register will identify all sensitive information assets, together with those information assets that are business critical, thereby allowing prioritsation of any risks and the allocation of resources. A senior officer has been assigned as the responsible information asset owner to each information asset. This will help the Council to mitigate against risks associated with particularly sensitive and vulnerable assets and move the Council towards full compliance with national legislation and regulations such as the Data Protection Act and the Re-Use of Public Sector Information Regulations. It will also ensure that the Council is following Local Government Association (LGA) guidelines.

3.10 Whilst the Information Asset Register provides a compendium of information assets and identifies owners for each information asset, the Council requires a Senior Information Risk Owner (SIRO) who has ultimate responsibility for the acceptance or otherwise of information risks for the Council, and will provide the Chief Executive with an annual statement of internal control for these assets. To this extent Corporate Leadership Team on 8th February endorsed a decision to appoint the Assistant Chief Executive (Planning, Policy and Improvement) to undertake this role for the Council.

3.11 As reported to Corporate Governance and Audit Committee in last year's report, the Council has strengthened governance arrangements by replacing the Information Governance Group with the Information Governance Management Board. The Information Governance Management Board (IGMB) is chaired by the Chief Officer for Business Transformation and is responsible for the development and overseeing the delivery of information governance across the Council. The IGMB is supported by a number of sub-groups that have responsibility for developing and implementing policy and practice for specific information governance areas, one of which has specific responsibility for information assurance.

3.12 A strategy for Information Assurance is being drafted that will set out how the Council will meet its information management and security responsibilities ensuring that all information is handled and stored with due regard to its value and risk. As part of this strategy a methodology is being designed that will seek to proactively identify threats to information security, and determine and action the most effective mitigations against such risks before they have the potential to become serious security incidents. The Council will use a Central Government model to benchmark progress it makes in developing and implementing good information assurance practice. The Model will assist the Council establish a comprehensive programme of work that will implement best practice and provide effective compliance across the Council.

3.13 In addition to improving the management of information assets, the growing need for the Council to share information in response to significant government reforms and the reconfiguration and joining up of local public services means that common standards need to be applied across the public sector. To this extent the Council is a signatory to the West Yorkshire Information Sharing Protocol which will be used as the basis for information sharing across the Council. The protocol has been developed in association with other West Yorkshire authorities in order to adopt a common and consistent approach to the sharing of information across the region.

3.14 The Council has agreed to adopt the Government Protect Marking Scheme (GPMS) as the security classification scheme that will protect and safeguard it's information assets, particularly when sharing information with external partners and organisations. To support the roll out of protective marking across the Council, there will be a programme of training & awareness for all staff. In order to effectively embed protective marking this needs to be underpinned with a technical solution to ensure users apply protective markings appropriately and consistently when creating emails and documents. GPMS is critical to the successful delivery of the EDRMS across the Council, and as such a decision has been taken to deliver protective marking across the Council via the EDRMS project. Discussions are ongoing with the EDRMS supplier, E2E, about whether their solution can automatically protectively mark documents and emails.

Skills and Competencies

3.15 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.

3.16 Discussions have been ongoing throughout the year with all Chief Officer's for Resources and Strategy (CORS) about identifying a resource within each Directorate who will be a contact for providing advice and guidance about information assurance and who will coordinate delivery of the information assurance strategy, and associated policies. Whilst progress is still to be made in some areas, most Directorates now have a nominated officer to undertake this role.

3.17 Furthermore, a training programme is being developed to ensure that the newly established roles within Directorates have the requisite skills and competencies to be able to carry out and conduct their responsibilities.

3.18 The responsibility for ensuring continued access to the Government Connect Security Extranet (GCSx), and the connection to other secure networks such as N3 for Health and the Public Sector Network now sits with the Information Governance Management Board. Whilst Corporate ICT Services are responsible for ensuring the technical infrastructure is in place to share information securely, it is the Business Transformation Team's responsibility for ensuring operation and maintenance requirements are maintained for Government Connect and new requirements are met for connection to other secure networks.

3.19 To this extent an existing FTE post on the Business Transformation Team establishment leads on work to ensure the Council complies with the applicable Government Connect Code of Connection controls, and to developing work to ensure connection to other secure networks. This post reports to the Corporate Information Compliance Manager.

Technology

3.20 The ICT Services Security team continues to develop and commission the strategic network defense elements identified within the PCI-DSS and GCSx compliance requirements, and strengthen the council's network against possible threats. Significant progress has been made over the last year, with the council accrediting to the new Code of Connection for GCSx, version 4.1. Highlights have included the following.

- The LogRhythm Security Information and Event Management (SIEM) device is now fully operational and active. It is actively monitoring the PCI-DSS and GCSx environments, providing protection to file integrity for these critical systems. It is also monitoring host attacks, including authenticated password failures, which may be indicative of a brute force attack, and providing automated warnings of such events. A dashboard is also available for continuous monitoring of the council systems.

- The new Web Gateway has now been rolled out across all users. It now enforces the council policy of preventing the download of executable files (.exe) and using its file type mismatch capabilities prevents the spoofing of other file type. Downloads are scanned for viruses and web connections to websites monitored for virus infection.

- Host Data Loss Prevention (HDLP) has been installed on all host computers including desktops and laptops. This is compiling details on all equipment attached to these devices and is ready to enforce policy on, for example, the use of unencrypted USB sticks.

- The Network Intruder Protection System (IPS) in now installed in the network and is enforcing the PCI-DSS policy. Intruder detection is now also active within the network monitoring and preventing virus attacks.

- Host Intruder Prevention Software (HIPS) has been deployed across all laptops and will be used to detect unauthorized access to computer resources, and to block certain undesirable applications such as toolbar and fake anti virus programs.

Work continues with additional defenses, such as McAfee Vulnerability Manager which is due to come on stream later this year.

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 2011/12.

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, training, 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

Information Governance Framework

SC Magazine

Information Security Report to Corporate Governance and Audit Committee 17th March 2010

Appendix A

Policy	Overview	Implications for Members	Current Progress
Information Security Policy	The purpose of the policy is to provide a framework to govern rules and procedures that determine the Council's commitment to ensuring that the confidentiality, integrity and availability of its information assets are protected and that all information is handled and processed securely. The Information Security Policy applies to information in all its forms, including, but not excluded to: • Paper • Electronic Documents • E-Mails • Voicemail • Web 2.0 records such as wikis, blogs and discussion threads • Visual images such as photographs • Scanned images • Microform, including microfiches and microfilm • Audio and video tapes, dvds and cassettes • Published web content (Intranet, Internet, Extranet) • Databases This policy will also apply to any information created in any other format that may be introduced or used in the future. The policy includes information transmitted by post, by person, by electronic means and by oral communication, including telephone. The policy applies throughout the lifecycle of the information from creation, through storage, utilisation to its ultimate disposal. With regard to electronic information systems, it applies to use of Council owned facilities and privately/externally owned systems when connected to the Council network directly or indirectly. The policy is supported by a set of standards, baselines, sub-policies, procedures and guidelines addressing individual aspects of security.	Ensure people's personal and/or sensitive information is kept secure in your house and when travelling around Ensure your laptop/computer/PDA password isn't written down anywhere Don't disclose personal and/or sensitive information without consent of the owner unless there is a lawful reason to do so Shred documents with sensitive information on or place in the confidential waste bins in the council Always keep council equipment secure when out of council premises Members Management System - Ensure information on the system is accurate, up to date and not kept for longer than necessary - Don't give others access to MMS You can only store council information on council equipment and systems	Undertaken consultation throughout the Council. Signed-off by Senior Information Risk Officer (SIRO) in December 2010.
Information Sharing	The Council is committed to working in partnership with other agencies involved in providing services to the public. It is recognised that the exchange of relevant information between such bodies is fundamental to achieving an effective	Don't disclose personal or confidential information to someone without consent of the owner unless it's lawful do to so. Ensure that persons receiving the information are authorised to	This policy is drafted and is currently going through consultation with officer

Policy	Overview	Implications for Members	Current Progress
	quality service. This policy provides a framework for the management of information sharing between the Council and other agencies and organisations.	do so including relatives, other organisations, councillors and services. Ensure you abide by information sharing agreements between agencies	groups. Due to be considered by the Information Governance Management Board in March 2011.
Information Risk Management	This policy will be developed once the Information Assurance Strategy for the Council has been approved. It will set out the regime for managing risks to information assets across the Council.	Not known at this stage	This policy is subject to the Council approving the Information Assurance strategy, which is currently in draft form. If the Council adopts this strategy and therefore a risk management approach to its information assets, the Information Risk Management policy will be drafted.
Information Incident Management	It is the policy of Leeds City Council, that all breaches of information security, actual or suspected, will be reported to and investigated by appropriately trained individuals within the council. In order to achieve this: • All users must immediately report all information security incidents and events, or suspected information security weaknesses. • It is prohibited for users to test any information security weaknesses without the cooperation and involvement of ICT Services. • All users must not disclose the details of any information security incidents to non□contracted third parties without explicit management authorisation. • Formal information security incident management procedures, including a method of incident categorisation based upon type, impact and severity levels, must be developed to ensure a timely, effective, and managed response to information security incidents. All reports of security incidents or violations of information security policy must be documented and include a review process in order to identify root causes, define any required preventative improvements and coordinate appropriate training and awareness sessions within the Council.	Email of call the ICT Helpdesk if you lose sensitive information or equipment. Incidents include - losing information	This policy is drafted and is currently going through consultation with officer groups. Due to be considered by the Information Governance Management Board in March 2011.

Policy	Overview	Implications for Members	Current Progress
Protective Marking & Asset Control	This Policy sets out appropriate measures through which the Council will classify its information, using the Government Protective Marking Scheme, to facilitate the secure handling, storage and disposal of its information assets. The policy also underpins the more effective and efficient information sharing with other public authorities who already apply protective marking such as the NHS, Police and Fire Service.	Documents and emails will be labelled with a security classification – Protect, Restrict, Confidential, Not Protectively Marked. You will have to apply this classification to certain documents in order to share information with agencies. This will mean a change to the email system which means that emails with confidential information in them with require extra buttons to be pressed on the email system before sending them	Undertaken consultation throughout the Council. Signed-off by SIRO in December 2010.
Information Systems Acceptable Use	The overall purpose of this policy is to provide protection for information assets owned and used by Leeds City Council from the risks posed by inappropriate use. This policy applies to everyone who has access to the council's information, information assets or IT equipment. The policy relates to the acceptable use of information and information systems, including future technologies. Information systems include any system for storing, , processing or communicating information. Information includes records, text, sound, images and moving images. This policy is part of a set of information governance policies and procedures that supports the delivery of the Information Governance Framework.	You won't be able to download your own software onto council computers and laptops Special software in ICT will be monitoring your internet usage.	This policy is drafted and is currently going through consultation with officer groups. Due to be considered by the Information Governance Management Board in February 2011.
Data Protection	This policy sets out our commitment to protecting personal data and how we implement that commitment with regards to the collection and use of personal data.	Ensure people's personal information is kept secure in your house. 1Personal data shall be processed fairly and lawfully 2Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes. 3Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. 4Personal data shall be accurate and, where necessary, kept up to date. 5Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or	This policy is drafted and is currently going through consultation with officer groups. Due to be considered by the Information Governance Management Board in February 2011.

Policy	Overview	Implications for Members	Current Progress
		those purposes. 6Personal data shall be processed in accordance with the rights of data subjects under this Act. 7Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.	
Freedom of Information & Environmental Information Regulations	The purpose of this policy is to ensure that the provisions of the Freedom of Information Act 2000 and the Environmental Information regulations are adhered to.	How to spot a Freedom of information request and what to do with it	This policy is drafted and is currently going through consultation with officer groups. Due to be considered by the Information Governance Management Board in February 2011.
Records Management	The purpose of this policy is to provide a single framework to ensure that a records management function is established within the council. This will ensure that records are managed in a way that supports the sharing of knowledge and information. Moreover this policy and subsequent best practice guidance will more easily allow the council to comply with its statutory obligations, mainly under the Freedom of Information Act 2000 and the Data Protection Act 1998.	Don't keep information for longer than you need it for. Check out if certain information has a set period for retaining it.	The existing policy is under review and going through consultation with officer groups. Due to be considered by the Information Governance Management Board in February 2011.
Remote Access	This policy sets out high level controls and is designed to ensure secure and resilient remote access to the council's information systems.	Unknown at this stage	This policy is currently being drafted by ICT Services, before going through officer groups for consultation.
Clear Desk & Clear Screen	The overall purpose of this policy is to ensure users have an awareness of the importance of keeping both paper and electronic documents and records safe when they are working at their desk/workstation or on their screen and that they have knowledge of how to protect them. This policy applies to everyone who has access to the council's information,	If you have a desk in the council & at home you must ensure it is cleared of council information when not in use by yourself.	Undertaken consultation throughout the Council. Signed-off by SIRO in December 2010.

Policy	Overview	Implications for Members	Current Progress
	information assets or IT equipment, whether office based or working remotely.		
Removable Media & Mobile Computing	This policy establishes the principles and working practices that are to be adopted by all users in order for information to be safely stored and transferred on removable media and mobile computing devices.	Use a council encrypted memory stick if you have to use one	Undertaken consultation throughout the Council. Signed-off by SIRO in December 2010.
Legal Admissibility	This policy will establish guidelines for legal admissibility of scanned, stored and electronically communicated data	Unknown at this stage	To be drafted once consultation with EDRMS supplier has taken place. Policy dependent upon how EDRMS operates.
Scanning	The purpose of the Policy is to: • Provide guidance on process, procedure and audit in order to ensure authenticity, integrity, security and maximum evidential weight of scanned, stored and migrated information • Improve reliability of, and confidence in, communicated information, and electronic documents to which an electronic identity is applied • Provide confidence to external inspectors (i.e. regulators and auditors) that the council's information and business practices are robust and reliable	Unknown at this stage	To be drafted once consultation with EDRMS supplier has taken place. Policy dependent upon how EDRMS operates.
Records Retention & Disposal	This policy sets out the principles behind records retention and disposal so that records are not kept for longer than they are needed, and in compliance with the Council's record retention schedules.	Unknown at this stage	The existing policy is under review and going through consultation with officer groups. Due to be considered by the Information Governance Management Board in February 2011.
Data Quality	To ensure that all council employees, concerned with data collection, are aware of the importance of recording and maintaining good quality data. Staff are obliged to maintain accurate records legally (Data Protection Act), contractually (Contract of Employment), and ethically (professional code of practice).	Member Management System Get it right first time when entering data onto the system, accuracy will help you Try and put information on as soon as you get it Double check after you've inputted people's details that they are correct Check that what you've entered onto the system is accurate.	This policy is drafted and is currently going through consultation with officer groups. Due to be considered by the Information Governance Management

Policy	Overview	Implications for Members	Current Progress
			Board in March 2011.
Remote Working	The purpose of this policy is to provide a framework for managing remote working and to reduce the level of risk posed by remote working to the lowest possible level. It sets out the requirements for legal compliance and the Council's duty of care.	Don't be a target – Keep your laptop covered when walking around – use a laptop bag or rucksack Place documents, laptops and memory sticks/data CDs in your boot when travelling by car You can only store council information on council equipment and storage	Policy signed – off. Policy owned by HR.