INFORMATION RISK MANAGEMENT INFORMATION SECURITY POLICY

KEY MESSAGES

Information security and the Information Security Management System (ISMS) are is intended to be enabling mechanisms for essential activities of the County Council such as information sharing, partnership working, remote and mobile working, for e-commerce and for reducing information-related risks to acceptable levels.

PURPOSE OF THIS POLICY

Lancashire County Council is committed to preserving the confidentiality, integrity and availability of all its physical and electronic information systems and records in order to provide assurance that the organisation manages information risk

- so that the needs of service users and citizens and the requirements of corporate governance and are met;
- to establish confidence that partnership arrangements involving sharing and exchange of information are legal and secure
- to establish that designed and implemented security features are effective
- to provide confidence that services & products offered by third party suppliers manage information risks on behalf of Lancashire County Council in a way which is adequate and fit for purpose;

Non-compliance with this policy could have significant effects on service delivery and may adversely impact individuals, waste resources and cause reputational damage to the County Council.

THE POLICY

Specific requirements for information security are contained in specific, documented policies and procedures. In particular, it is the Policy of Lancashire County Council to ensure that

- Information will be protected against unauthorised access
- Confidentiality of information will be assured1
- Integrity of information will be maintained2
- Regulatory and legislative requirements relevant to information systems will be met3
- Business Continuity Plans will be produced, maintained and tested4
- Information Security Training is available to all staff. All staff must undergo the information assurance e-learning course and annual refresher courses.
- All breaches of Information Security, actual or suspected, will be investigated and reported to the Corporate Information Assurance Manager

Disciplinary action may be considered in the event of breaches of this policy.

---

1 The protection of sensitive or valuable information from unauthorised disclosure or intelligible interruption or theft
[2] Safeguarding the accuracy and completeness and authenticity of information by protecting against unauthorised modification of information and systems
[3] This includes, among others, the requirements of the Data Protection Act and external requirements such as NHS Codes of Connection
[4] This will ensure that information and vital services are available in a useable form to users when and where they need them

SCOPE

This policy applies to

- All employees and elected Members of the County Council and other non-employees granted access as users of LCC information systems are expected to comply with this policy and with the ISMS that implements this policy as appropriate to their work roles.
- All information and records in all formats and media including electronic records, paper records, photographs, recorded conversations, voicemail and CCTV images which are produced by Lancashire County Council.
- All systems, processes and guidance designed or employed to administer, store or protect the information assets held by the Council.
- This policy applies throughout the lifecycle of all information from creation through storage and use to disposal.

SPECIFIC REQUIREMENTS

Detailed Information Security Policies
All Council staff and third parties engaged on LCC business must abide by detailed security policies as appropriate to the circumstances of their work. All staff must sign the agreement for Acceptable Use of Internet, Email & telephones and the acknowledgement of having read Policy 9 Information Handling.

1. Acceptable Use Policy
2. Training and Awareness Policy (76 KB, Word Document)
3. Personnel Policy
4. Secure Technical Infrastructure Policy
5. Local Information Risk Policy
6. Security in New Business Processes
7. Critical Business System Policy
8. Information Classification Scheme
9. Information Handling Policy
10. Incident Management and Reporting
11. Business Continuity Policy
12. Legal Obligations Policy
13. Data Protection Policy
14. Records Management Policy
15. Physical and Environmental Security Policy
16. Tier 0 North West Statement
17. Tier 1 Information Sharing Code of Practice
18. Tier 2 Information Sharing Protocol Template
19. Policy for Secure Disposal of Physical Records
20. Encryption Policy

Link: http://lccintranet2/corporate/web/view.asp?siteid=4305&pageid=27633&e=e

Legal Compliance

All Council staff and third parties engaged on LCC business must abide by all UK and European legislation, which is relevant to the security of its information. This legislation includes but is not limited to:

1. Data Protection Act (1998);
2. Freedom of Information Act (2000);
3. Human Rights Act (1998);
4. Civil Contingencies Act (2004);
5. Common Law Duty of Confidentiality;
6. Computer Misuse Act (1990);
7. Copyright, Designs and Patents Act (1988);
8. Electronic Communications Act (2000);
9. Regulation of Investigatory Powers Act (2000).

Link: http://lccintranet/corporate/data_protection/index.asp and
http://lccintranet/corporate/freedom_of_info/index.asp

Information Management Practices contributing to Information Security

Good information security depends on good information management practice. This policy therefore requires that the following general information management measures are in place.

- Asset Management – all assets (information, hardware and software) must have an "owner" who is responsible for
    - the maintenance and protection of the asset concerned.
    - classification of information associated with the asset according to its sensitivity
    - completion of a statement of conformity to the Data Quality Strategy (for major assets).
    - all assets should be recorded and managed either though the Information audit, a software portfolio or a hardware inventory
- Human Resources – HR practices should take into account information security as follows
    - Job descriptions should set out relevant security responsibilities and screening processes.
    - The Information Assurance e-learning courses must be successfully completed before any new staff member is granted access to Council information systems holding personal or sensitive data.
    - Upon change or termination of employment all ICT equipment must be returned to Lancashire ICTS Services and all access rights revoked.
- Physical and Environment Security - Physical security and environmental conditions must be suitable to manage the risks to information assets. Owners of assets should work with Premises Managers to ensure that the physical security of their local operating environments are assessed and protective measures or compensating controls put in place according to the value of and risk to assets.
- Operations Management – While information Asset owners remain responsible for services and information content directly connected with those services, all information systems, whether existing or proposed, must be managed within the support framework provided by corporate policies, ICT policies, cross directorate contracts and other support services such as ICT Services, Record Management Services, CIGG, Access to Information Team and Property Group.
- Access Control - Access to information and to information systems must be granted only to a level that will allow users to carry out their role and must not be excessive to the requirements of that

role and access rights must be kept current. Access to information assets must be governed by a formal process covering
    - Screening and/or training of employees
    - User registration and de-registration procedures covering starters, leavers and internal changes to responsibilities
    - Positive authorisation for access to particular assets by the asset owner.
- Information shared with a partner, supplier or third party contractor should be subject to an Information Sharing Agreement or Third Party Data Processing Contract.
- Business Continuity - Service continuity planning for ICT systems will be carried out by Lancashire ICT Services, but the business areas will be responsible for the business continuity plans for the services they provide.
- Information security incidents and weaknesses must be recorded and mitigating action taken in a consistent and timely manner. All security incidents should be reported using the e-form provided on the Information Governance intranet pages.

RESPONSIBILITIES

- The Senior Information Risk Owner (SIRO) owns the Council's overall risk in the sense of monitoring relevant risk and developing policy to mitigate this risk.
- The Corporate Information Governance Group are responsible for supporting the SIRO by developing and promulgating this Policy, providing relevant advice and guidance to managers, staff and other users, including provide mandatory annual information assurance e-learning refresher courses for all staff and working in liaison with ICTS, Records Management and other staff to develop the Information Security agenda.
- Managers in each Directorate are responsible for ensuring that their staff follow the prescribed guidance in this area, and shall be responsible for the security of the information assets, systems, equipment, information and records within their areas. Managers shall attend an annual information risk review workshop to assess their level of risk each year. They shall be given actions and advice on how to improve their risk rating which they can incorporate in the form of an action plan that can be imbedded in their business planning processes.
- Operational Managers must work with Information Governance staff, ICT technical staff, Premises Managers, Audit, HR and any other relevant support staff where this is relevant to managing information risk.
- All staff and other users are responsible for ensuring due care for the systems, equipment, information and records with which they work, and shall observe the provisions of this Policy and all the guidance which is produced in support of it within other relevant information governance framework policies and procedures.

VIOLATIONS

Compliance with this policy and its supporting guidance is mandatory and must be observed on all County Council business

As an enabling mechanism, failure to demonstrably implement this policy may cause serious operational problems especially in the areas of information sharing, partnership working, remote and mobile working, for e-commerce.

In the event of an incident where a breach has an adverse impact on individuals through unauthorised disclosure, loss or corruption of personal data, the Information Commissioner may, depending on the seriousness of the impacts, take actions ranging from undertakings to comply with the Data Protection

Act, through enforcement notices or Civil Monetary Penalties (up to £500k) and criminal prosecutions against responsible individuals and organisations.

Title	Information Risk Management Information Security Policy
Aim	To provide staff with responsibilities with high level guidance of the standards expected for the management of information risk and information security with an indication of their scope and applicability.
Authored/developed by	Frank Loughlin(IG),
Circulated to	CIGG
Responsible Director	Bill Brown, SIRO
Date Ratified	Not yet ratified
Ratified by	CIGG
Implementation Date	
Review Period	Annual
Next Review date	Ratification date +12 months

Document Control

Date	Author	Version	Change Description	Document Status
December 2010	F. Loughlin, D. Bonser	1.0	Initial document	Draft

This document is uncontrolled when printed. To ensure that you have the current version, please visit the Information Governance site at http://lccintranet2/corporate/web/view.asp?siteid=4305&pageid=27633&e=e