INFORMATION & KNOWLEDGE MANAGEMENT

Leeds CITY COUNCIL

LEEDS CITY COUNCIL

INFORMATION SECURITY POLICY

INFORMATION & KNOWLEDGE MANAGEMENT

DOCUMENT CONTROL

Version History

Version	Status	Revision Date	Summary of Changes	Author
0.01	Draft	28th April 08	Original draft version	AN
0.02	Draft	10th July 08	Changes due to comments from Principal IT Officer (IT Security)	AN
1.0	Draft	18th Aug 08	Change due to comments from MT	AN
2.0	Draft	17th Sep 08	No Changes received from CGB	AN
3.0	Draft	7th Nov 08	Changes due to comments from Govt Connect Board	AN
4.0	Draft	25th Nov 08	Changes due to comments from Head of Governance Services	AN
5.0	Draft	11th Dec 08	Changes due to comments from Assistant Chief Executive (Planning, Policy and Improvement)	AN
VR1	Final Draft	16th Dec 08	Changes due to further comments from Assistant Chief Executive (Planning, Policy and Improvement)	AN
VR2	Final	19th Dec 08	Delegated Decision Notice Approval by Assistant Chief Executive (Planning, Policy and Improvement)	AN

Approvals

Name	Signature	Title	Approval Details	Date
IGAG			Meeting of the Group	18th Aug 08
CGB			Meeting of Board	17th Sep 08
Assistant CX (Planning, Policy and Improvement)			Delegated Decision Notification	19th Dec 08

Review/Consultation

Name	Signature	Title	Approval Details	Date
IGAG				18th Jul – 15th Aug 08
Corporate Governance Board				17th Sep 08
Government Connect Programme Board				23rd Oct 08
Assistant Chief Executive (Planning, Policy and Improvement				11th Dec 08

Distribution List

Name	Title	Date of Issue	Version

Alistair Fletcher	IT Security Officer		
Review Panel	IKM & ICT	14th July 08	0.02
Kate Dover	GC Project Officer	14th July 08	0.02
Chris Blythe		14th July 08	0.02
IGAG		18th July 08	1.0
CGB		17th Sep 08	2.0
Govt Connect Prog Board		23rd Oct 08	3.0
IKM		25th Nov 08	4.0
Assistant Chief Executive (Planning, Policy and Improvement)		27th Nov 08	5.0

Document References

Document Name	Document File Path

INFORMATION & KNOWLEDGE MANAGEMENT

1. Introduction

This policy should be read in conjunction with the Records Management Policy.

The Council recognises that information and information systems are valuable assets, which play a major role in supporting the organisations strategic objectives. Information security is important for ensuring the safe and secure transaction of information for Council business and the success of carrying out policy and administrative activities.

Information security is an integral part of information sharing, which is becoming increasingly important to achieving Council aims and objectives. The management of personal information has important implications for individuals and is subject to legal obligations under the Data Protection Act 1998. The consequences of information security failures can be costly, potentially embarrassing and time-consuming.

The Information Security Policy sets out appropriate measures through which the Council will facilitate the secure and reliable flow of information, both within the Council and in external communications. It comprises this document, which sets out the principles and framework, and a set of standards, baselines, sub-policies, procedures and guidelines addressing individual aspects of security (listed in Appendix A).

This policy is based on recommendations contained within the International Standard on Information Management Security Systems 27001.

2. Objectives

To ensure that all information and information systems upon which the Council depends are adequately protected to the appropriate level.

To ensure that all staff have a proper awareness, concern and an adequate appreciation of their responsibility for information security.

To ensure that all contractors and their employees, temporary staff and other visitors likely to use and process Council information have a proper awareness and concern for security of Council information.

To provide a framework giving guidance for the establishment of standards, baselines, sub-policies, procedures and guidelines for implementing information security.

To meet the general objectives of ISO-27001 Code of Practice for Information Management Systems Security.

To ensure that all staff have an awareness of their responsibilities for processing personal information under the Data Protection Act 1998.

To ensure that all staff are aware of their accountability and that they are aware that failure to comply with the requirements of the Information Security Policy is a disciplinary offence and will be considered in accordance with the Council's disciplinary procedure.

3. Purpose and Scope

The purpose of the policy is to provide a framework to govern rules and procedures that determine the Council's commitment to ensuring that its information assets are protected and secure.

The Information Security Policy applies to information in all its forms, including,

- 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 documents created in any other format that may be introduced or used in the future.

The policy covers 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.

Appropriate protection is required for all forms of information to ensure business continuity and to avoid breaches of the law and statutory, regulatory or contractual obligations.

The policy applies to all officers and Council Members and to other users associated with the Council. 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.

4. Policy Statement

The Council recognises the importance of its information assets and the need for proper, effective management of information systems within the organisation. It is important that there is in place sufficient and adequate information security safeguards and countermeasures to provide the continued security of Council information. The Council is committed to protecting the security of information through the preservation of:

- Confidentiality - protecting information from unauthorised access and disclosure;
- Integrity – safeguarding the accuracy and completeness of information and processing methods;
- Availability – ensuring that information and associated services are only available to authorised users when required.

5. Legal Requirements

Information Security sits within a legislative background and a number of Acts of Parliament and international standards influence this policy. Appendix B provides further information.

6. Information Security Policy Principles

The information creation, storage, maintenance, retention and disposal processes are informed by the Council's Records Management Policy and should embody the following principles of information security:

- Measures taken or installed are appropriate to the level of security required to maintain the confidentiality and integrity of information;
- Staff should be able to access information for the effective performance of their role;
- Information security should not create a barrier to the flow of information across the Council, but should provide appropriate controls and permissions;
- All users should be accountable for their use of information in line with the information security policy;
- Information management must comply with prevailing legislation;
- Personal, confidential and sensitive information must be protected;
- Information must be managed in accordance with agreed security procedures;
- Information must be classified according to an appropriate level of availability (See Appendix C for example);
- Data backup and recovery and business continuity plans are tested and maintained to ensure that vital information services are available within defined service levels;
- Breaches of information security controls will be reported to and will be investigated by an officer who has been assigned information compliance responsibilities;
- All users will comply with the Copyright, Designs and Patents Act 1988 under which it is an offence to copy software or licensed products without the permission of the owner of the copyright;
- Users will consider security when using and disposing of information. Staff should refer to the Council's Records Retention and Disposal Policy, and ensure that all information is covered by an appropriate retention period and follow established procedures for the disposal of information safely and securely;
- All Council computer hardware must be disposed of in accordance with the Council's Records Retention and Disposal Policy, and;
- Compliance with this policy will be enforced.

7. Policy Framework

7.1 This policy is a framework by which Information Security will be adopted, implemented and embedded across the Council. The policy will be supported by a series of other standards, rules, sub-policies, procedures and guidelines that will form the basis of the Council's Information Security Management System.

7.2 Appendix A outlines the standards, rules, sub-policies, procedures and guidelines that will form the basis of the Council's Information Security Management System.

8. Roles and Responsibilities

8.1 All staff have a duty of care to protect and ensure the security of the Council's information assets. Everyone granted access to the Council's information systems has a personal responsibility to ensure that they, and others who may be responsible to them, are aware of and comply with this policy and supporting policies, procedures, standards and guidance.

8.2 There will be some specific responsibilities as detailed below:

Assistant Chief Executive (Planning, Policy and Improvement)

The Assistant Chief Executive (Planning, Policy and Improvement) will be responsible for;

- Approving this policy;
- Supporting the implementation and enforcement of this policy and supporting documents.

Corporate Governance and Audit Committee

The Corporate Governance and Audit Committee will be responsible for reviewing this policy in line with the Council's corporate governance framework.

Corporate Governance Board

Corporate Governance Board will ensure the policy is appropriate to fit with the overall governance framework of the Council.

The Information Governance Group

The Information Governance Group will be responsible for:

- Contributing to the development of, and reviewing, this policy;
- Advising on appropriate methodology for ensuring full implementation of this policy across the organisation;
- Coordinating the development of other policies, standards, guidelines and procedures for the implementation of this policy, and;
- The on-going review of the effectiveness of this policy and supporting policies, standards, guidelines and procedures.

Information and Knowledge Management Team

The Information and Knowledge Management Team will be responsible for:

- Developing, maintaining and reviewing this policy, working with relevant corporate resources, for producing associated policies, standards, guidelines and procedures;
- Establishing and maintaining a corporate register of the Council's information sharing agreements;
- Providing advice and assistance on the development of information sharing agreements;

- Developing a corporate strategy for information security and information sharing, coordinating implementation, dissemination and monitoring operation;
- Coordinating the work of the officers assigned responsibility for Information Compliance in Directorates;
- Representing the Council at regional and national assemblies and events strategic issues relating to information security, and;
- Ensuring that staff receive training appropriate to their information security needs, and in particular the Data Protection Act 1998 in relation to personal data.

Chief Officers Resources and Strategy (or other officers nominated by the Director/Assistant Chief Executive)

The Chief Officers Resources and Strategy (or other officers nominated by the Director/Assistant Chief Executive) will be responsible for:

- Advising, identifying and commissioning appropriate support resources to ensure this policy is implemented and embedded throughout the organisation;
- Ensuring that staff are fully informed of their obligations and responsibilities with respect to this policy and associated policies, standards, guidelines and procedures;
- Ensuring that information security incidents or concerns are brought to the attention of the an appropriate officer assigned responsibility for Information Compliance at the earliest opportunity, and;
- Ensuring that temporary staff or external contractors only access information required to perform their duties with the Council and are provided information security training before handling any Council information.

Information Compliance Officers (or officers assigned responsibilities for Information Compliance

The Information Compliance Officers (or officers assigned responsibilities for Information Compliance) working within the Directorates will be responsible for:

- Facilitating the implementation of this policy through appropriate policies, standards, guidelines and procedures;
- The investigation and logging of all security breaches within their Directorate and reporting the incident(s) to the appropriate resource;
- Monitoring that information sharing agreements are in place and up-to-date and for ensuring that these are recognised and embedded within the culture of the Directorate, and;
- Acting as a point of contact within the Directorate for issuing advice and guidance on information security issues.

Corporate ICT Services

Corporate ICT Services will be responsible for:

- Providing technical advice;
- Managing the necessary technical environment and tools to support the implementation, delivery, monitoring, auditing, testing and review of the policy, and;
- Overseeing, monitoring, auditing and testing technical compliance to the policy.

Individual Employees

Each employee is responsible for:

- Protecting the Council's information assets, systems and infrastructure, and will protect likewise the information assets of third parties whether such protection is required contractually, legally, ethically or out of respect for other individuals or organisations;
- Reporting any observed or suspected security incidents where a breach of the Council's security policy has occurred, any security weaknesses in, or threats to, systems or services, and;
- Complying with policy during day-to-day operations.

9. Training

9.1 Appropriate training will be made available for existing staff that have responsibility for information security duties.

9.2 All staff will be made aware of their obligations for information security through effective communication programmes.

9.3 Each new employee will be made aware of their obligations for information security during an induction-training programme.

9.4 Training requirements are reviewed on a regular basis to take account of the needs of the individual, and to ensure that staff are adequately trained.

10 Review and Maintenance

10.1 Ownership of the Information Security Policy is vested in the Information and Knowledge Management Team who are responsible for the maintenance and review of the policy.

10.2 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 and Knowledge Management Team, and interim information audits across the Council.

10.3 The policy will be reviewed on an annual basis by the Information Governance Group, or in response to any changes affecting the basis of the original security risk assessment, for example:

- significant security incidents;
- new vulnerabilities;

- changes to the organisational or technical infrastructure, and;
- changes to legislative requirements.

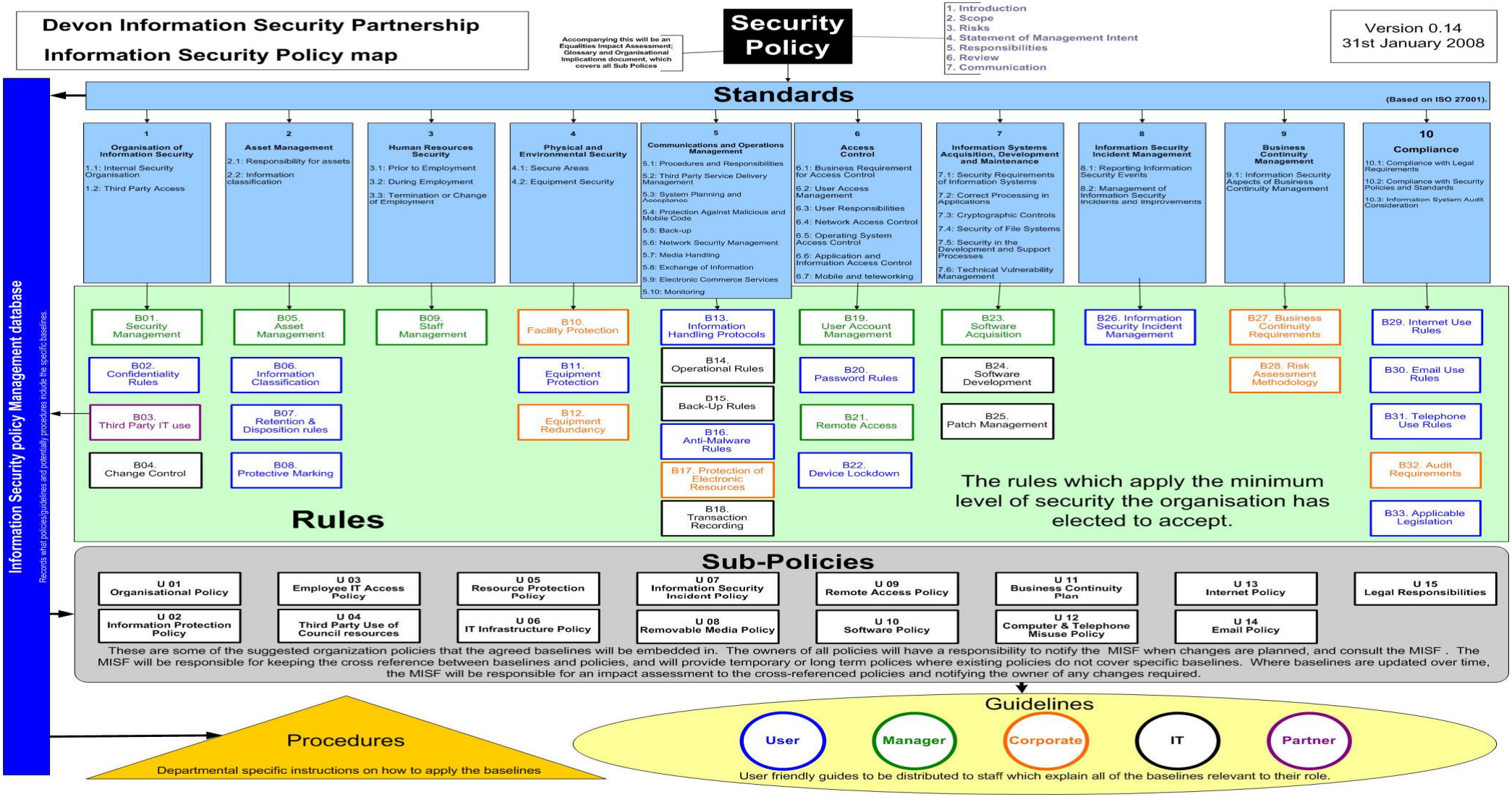
11. Declaration

11.1As part of the consultation process this policy has been endorsed by the Council's Information Governance Group and Corporate Governance Board. In accordance with the Council's Information Governance Framework this policy is formally adopted as a Council policy.

James Rogers
Assistant Chief Executive (Planning, Policy and Improvement)

INFORMATION & KNOWLEDGE MANAGEMENT

Appendix A



INFORMATION & KNOWLEDGE MANAGEMENT

Appendix B

Legal Requirements

Legislation	Context
Data Protection Act 1998	The purpose of this Act is to protect the rights of the individual about whom data is obtained, stored, processed or supplied rather than those of the employees of the Council who control and use personal data. The Act requires that appropriate security measures will be taken against unauthorised access to, or alteration, disclosure or destruction of personal data and against accidental loss or destruction of personal data.
Copyright, Designs and Patents Act 1988	The Act states that it is illegal to copy and use software without the copyright owners consent or the appropriate licence to prove the software was legally acquired.
Computer Misuse Act 1990	The Act states that it is a criminal offence to **attempt** to gain access to computer information for which you have no authorisation. On ending their employment with the Council, employees and contractors must not disclose information which was confidential.
Freedom of Information Act 2000	The Act gives everyone a legal right to see information held by public authorities. The aim is to open up public organisations to make the more accountable to the public.
Caldicott Report 1997	The Department of Health issued the Caldicott Report which dictates levels and standards for securing information and computer systems. The increase emphasis on Electronic Patient Record and Clinical Governance has heightened security awareness. The main objective of the report is to outline measures to maintain the security of patient-identifiable information.
Human Rights Act 1998	The part of the Act most relevant to Information Security refers to Article 8 of the European Convention on Human Rights. Personal data is part of an individuals 'private life' and as such they have the tight to have such information treated in the strictest confidence.
The Regulations of Investigatory Powers Act 2000	The Act regulates the power of government security services and law enforcement authorities by allowing the interception, surveillance and investigation of electronic data in specified situations such as when preventing and detecting crime.

Appendix C

Table of the Information Security Classifications

Example Only

Classification	Context
Unrestricted	Public information (including information deemed public by legislation or through a policy of routine disclosure). Available to the public, all employees, contractors, sub-contractors and agents.
Protected	Information that is exempt from release under the Freedom of Information Act 2000 and is sensitive outside the Council and needs to be protected. Authorised access to employees, contractors, sub-contractors and agents on a 'need-to-know basis for business related purposes.
Restricted	Information that is exempt from release under the Freedom of Information Act 2000 and that is sensitive within the Council and is available only to a specific function, group or role
Confidential	Information that is exempt from release under the Freedom of Information Act 2000 and is of a highly sensitive nature and is available only to specific, named individuals (or specific positions).