West Lindsey District Council

Information Security Policy

Document Control

Organisation	West Lindsey District Council
Title	Information Security Policy
Author	S M Anderson
Filename	
Owner	ICT Manager
Subject	Policy Document
Protective Marking	Not Protectively Marked
Review date	23 Jun 2015

Revision History

Revision Date	Revised By	Previous Version	Description of Revision
21/6/2011	Steve Anderson	Draft V0.1	Branding applied
2/9/2011	Steve Anderson	Draft V0.2	Para 4.5.1 amended to clarify applicability to elected members
29/9/2011	Steve Anderson	Draft V0.3	Adopted by Policy and Resources Committee
23/6/2014	Steve Anderson	Version 1.0	Reviewed by Corporate Information Governance Group. Para 4.1 revised. Approved by CMT.

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Date
Assistant Chief Executive	Alex Reeks	

Document Distribution

This document will be distributed to:

Name	Job Title	Email Address

1. Contents

2. Foreword by the Chief Executive

Information is the life blood of West Lindsey District Council. Without it, our jobs would be impossible to do. Information is precious. We are committed to preserving the confidentiality, integrity, and availability of our information assets:

- for sound decision-making;
- to deliver quality services to our customers;
- to comply with the law;
- to meet the expectations of our customers and citizens; and
- to protect our reputation as a professional and trustworthy organisation.

Damage to any information we hold can cause problems for our business, customers, citizens, and third parties. We have identified information management as one of our key risks and are putting in place measures that help us to manage it.

Information security is everyone's responsibility. We all need to make sure that we know how to use information safely and securely. This policy sets out what we all need to know. Whilst it is an important policy document, it is readable and full of practical help - please read it and ask yourself if you are doing everything you can to protect our reputation.

Manjeet Gill
Chief Executive
West Lindsey District Council

3. Introduction and Scope

3.1 Information is an important asset and of significant value to West Lindsey District Council (the council). The council must protect its information from threats, internal and external, deliberate or accidental, that could disrupt its work or infringe the rights of staff or customers.

3.2 Information security involves the protection of information for:

- **Confidentiality**: Making sure that information is accessible only to those authorised to have access.
- **Integrity**: Safeguarding the accuracy and completeness of information and processing methods.
- **Availability**: Ensuring that authorised users have access to information and associated assets when required.

3.3 All information created or processed on behalf of the council is regarded as being owned and accessible by it as part of the council's "business record".

3.4 This policy focuses on all types of information and security including:

- information systems;
- all paper records;
- microfiche, visual and photographic materials e.g. CCTV, slides;
- spoken conversation, including voicemail and recorded conversations; and
- the technology used to hold, process, transfer and transmit the council's information e.g. memory sticks.

3.5 The policy applies throughout the lifecycle of the information from creation through storage and use to disposal. All the controls required will be effective and appropriate; offering adequate protection without unnecessary expense or intrusion.

3.6 This policy is based on the International Standards for Security Management, ISO/IEC 27000 series.

4. Information Security Policy Statement

4.1 Aim of the policy

4.1.1 The overall aim of this policy is to reduce the risks, from whatever source, to the security of the council's information and that of its customers and partners. By doing this the policy will minimise potential damage to the council, its assets and its reputation, by preventing and reducing the impact of security incidents.

4.1.2 The Information Security Policy is in place to make sure that:

- the council establishes a culture of care for information held by the council and immediately report any incidents of loss;
- information is only obtained when it is required;
- information owned or processed by the council is protected against unauthorised access or use;
- Information and Communication Technology (ICT) equipment is protected from accidental or malicious damage;
- security risks are properly identified, assessed, recorded and managed;
- cost-effective safeguards are implemented to reduce security risks;
- appropriate monitoring and reporting processes are put in place to identify and act immediately upon breaches of information security;
- legal and regulatory requirements are understood and met; and
- information and training on information security is available and up-to-date.

4.2 Approach

4.2.1 This policy is based on an industry standard framework and the ISO/IEC 27000 series the International Standards for information security management. All recognise the need to match the Information Security Policy and its implementation to the security risk and the impact of a security breach.

4.3 *Application*

4.3.1 This policy applies to all employees, elected members, contractors, agents and representatives and temporary staff working for or on behalf of the council.

4.3.2 Aspects of this policy will be relevant to people the council share information with, such as voluntary organisations, agencies and partnerships, as part of the work of the council.

4.4 Roles and Responsibilities

4.4.1 The Chief Executive (CE) will bear responsibility for the security of the data and information.

4.4.2 The CE will do this through the Wider Management Team (WMT), which shall maintain a high-level overview of data and information security and shall report to the CE at intervals determined by the CE.

4.4.3 The Information Security Policy is developed in consultation with the People and Organisational Development department and the Joint Staff Consultative Committee (JSCC), and is formally approved by the Policy and Resources Committee (P&R Committee).

4.4.4 The ICT Manager is the designated owner of the Information Security Policy and is responsible through the WMT for providing direction for the management of information security.

4.4.5 Raising awareness of this policy shall be led by the Information Governance Officer and officers of the council within ICT and is the responsibility of all managers.

4.4.6 All service managers and team leaders are responsible for making sure that this policy is communicated within their service and that all their staff know about and understand their information security responsibilities.

4.4.7 It is everyone's responsibility to make themselves aware of the content of this policy and its sub-policies, and codes of practice, and to adhere to them (see Appendix A).

4.5 Breaches of the Policy

4.5.1 Breaches of this policy are regarded as a disciplinary matter and, in the case of a member of staff, those classed as gross misconduct may lead to dismissal. Breaches of this policy by an elected member are covered by the Member Code of Conduct and could be referred to the Standards Committee.

4.5.2 Any breaches, observed or suspected, of the Information Security Policy and sub-policies must be handled in accordance with the Information Security Incident Management Policy.

4.6 Policy Implementation

4.6.1 This policy will be made available to all staff (whether permanent or temporary), elected members and partners/agents and the key messages delivered through a dedicated communications campaign.

4.6.2 The council will provide corporate Information Security and Awareness training to everyone who accesses council information.

4.7 Policy Review

4.7.1 The current version of this policy and supporting sub-policies are held on the Intranet and can be made available to the public except where the council considers the disclosure of the sub-policy may lead to a compromise in security.

4.7.2 The policy will be reviewed every 12 months by the ICT Manager with the support of the Corporate Information Governance Group (CIGG) and within the appropriate consultation and approval process.

4.7.3 Any significant changes will be approved by the WMT and, if considered necessary, the JSCC and the P&R Committee. Changes will be communicated to all staff, elected members and agencies and partners. The corporate Information Security and Awareness training programme will be updated as appropriate.

5. Risk Assessment, Treatment and Management

5.1 The council shall provide protection to its information assets and systems where these assets are held, commensurate with their value and importance to the organisation. This is emphasised in the Risk Management Strategy and Framework.

5.2 Risks will be assessed and appropriate control measures put in place to reduce these risks. Guidance on risk assessments can be found in the Risk Management Strategy.

5.3 So that appropriate control measures can be put in place before their implementation or use, the business sponsor or system owner will assess the Information Security risk of:

- all new information assets and systems; and
- modifications or development of existing systems.

5.4 Having identified the risks, appropriate measures will be adopted to make sure systems and information are secure.

5.5 There must be periodic reviews of the identified security risks and related controls, taking accounts of new threats and vulnerabilities, to determine whether current controls are still effective.

5.6 Internal Audit can give an independent assurance on the controls implemented.

6. Organisation of Information Security (the Framework)

6.1 Appendix 1 illustrates a framework of policy and guidance that governs the operation of information security within the council:

6.2 The strategic direction of the council in matters of ICT and information security is towards full compliance with the International Standards ISO27000 Series.

6.3 The council and its employees and agents shall abide by all United Kingdom and European legislation which is relevant to the security of its information. Relevant legislation is listed in the Legal Responsibilities Policy (TBA) and includes:

- Common Law Duty of Confidentiality;
- Computer Misuse Act (1990);
- Copyright, Designs and Patents Act (1988);
- Data Protection Act (1998);
- Freedom of Information Act (2000);
- Human Rights Act (1998);
- Civil Contingencies Act (2004);
- Electronic Communications Act (2000);
- Regulation of Investigatory Powers Act (2000).

6.4 Where relevant to local government the council shall comply with the guidance contained in the National Information Assurance Strategy for Local Government. The current general version can be found at the cabinet Office web site:

http://www.cabinetoffice.gov.uk/csia/publications.aspx

7. Information and ICT Asset Management

7.1 Responsibility for assets

7.1.1 All assets (data, information, software and hardware) must be accounted for and have an owner. The owner shall be responsible for the maintenance and protection of the asset/s concerned.

7.1.2 Documented rules will be established and maintained for the acceptable use of information and assets associated with information processing facilities.

7.2 Information Classification

7.2.1 All information assets should be classified and protected in accordance with the council's Information Management and Protection Policy.

8. People and Organisational Development – recruiting, during service, leaving or transferring

8.1 Council employee, contractor and third party terms and conditions of employment/working and any supporting documents, e.g. job descriptions, must set out security responsibilities with an adequate screening and declaration processes in place. For more information please see the Human Resources Information Security Standards Policy (TBA).

8.2 Upon a change or termination of employment, clearly defined and assigned procedures must be followed at all times. These include the return of all council-owned assets and the revoking or amendments of the person's access rights. For more information please refer to the IT Access Policy.

9. Physical & Environmental Security

9.1 Physical security and environmental conditions must be suitable to manage the risks to the area concerned. In particular critical or sensitive information processing facilities must be housed in secure areas protected by defined security perimeters with appropriate security

barriers and/or entry controls and protection for the infrastructure. For more information please refer to the IT Infrastructure Security Policy.

9.2 Information, including electronic information and printouts produced from computer systems, must be stored and used in accordance with the principles of the Data Protection Act 1998 and any other legislation and council information and records management policies.

9.3 The council recognises, through its Flexible Working Policy and from its business requirements, that elected members, staff and agents need access to council information and systems from home or other remote locations. They also need to access information and communicate electronically using public networks such as the Internet. The following policy documents provide information and guidance on accessing council systems from outside the council's physical boundary and the acceptable use of the Internet and electronic communication services:

- Remote Working Policy
- Removable Media Policy
- Internet Acceptable Use Policy
- Email Policy

10. Communications & Operations Management

10.1 Responsibilities and procedures for the management, operation and ongoing security and availability of all information processing facilities within, outside and between the council and other partner or third party organisations must be established (see TBA).

10.2 Information must be stored and destroyed in a controlled manner.

10.3 A Records (Data) Retention and Disposal Schedule must be implemented for all information holding systems both manual and electronic.

10.4 For information about communications and operations management please refer to the Communications and Operations Management Policy (TBA).

11. Information and Systems Access Control

11.1 Access to information and information systems must be driven by business requirements. Access shall be granted to council staff, elected members, contractors and third parties to a level that will allow them to carry out their duties and shall not be excessive of their role.

11.2 A formal user registration and de-registration procedure is required for access to all information systems and services. This must include amendments when staff change roles within the council.

11.3 Necessary controls will be put in place before connecting third parties to any council ICT facilities after approval by ICT.

11.4 For more information please see the IT Access Policy.

12. Information Systems and Technology Management

12.1 Security is an integral part of information systems. Security risks and requirements must be identified at the earliest stage in the system development or acquisition cycle, along with controls to be implemented to mitigate the risks.

13. Information Security Incident Management & Monitoring

13.1 Information security incidents and weaknesses must be recorded and mitigating action taken in a consistent and timely manner.

13.2 All staff will be encouraged to report any security breach, actual or potential, without fear of recrimination.

13.3 All security incidents will be logged and investigated where appropriate.

13.4 Security incidents that result from a deliberate disregard of any security policy requirements may result in disciplinary action.

13.5 Detailed information on the council's policy on managing security incidents can be found in the Information Security Incident Management Policy.

14. Business Continuity Management

14.1 Arrangements must be in place for the timely resumption of business information systems in the event of a failure in these systems or damage to them arising from a disaster.

14.2 Service continuity planning for the ICT systems will be carried out by the ICT Department, but the business areas will be responsible for the business continuity plans for the services they provide.

14.3 The purpose of the plan is to reduce, to an acceptable level; the actual or potential disruption caused by, among other things, failures of information security.

14.4 Disaster recovery arrangements will be tested at least annually and will be reviewed and updated as areas of business risk are identified and business continuity arrangements are developed.

14.5 More details of business continuity management can be found at (TBA).

15. Compliance

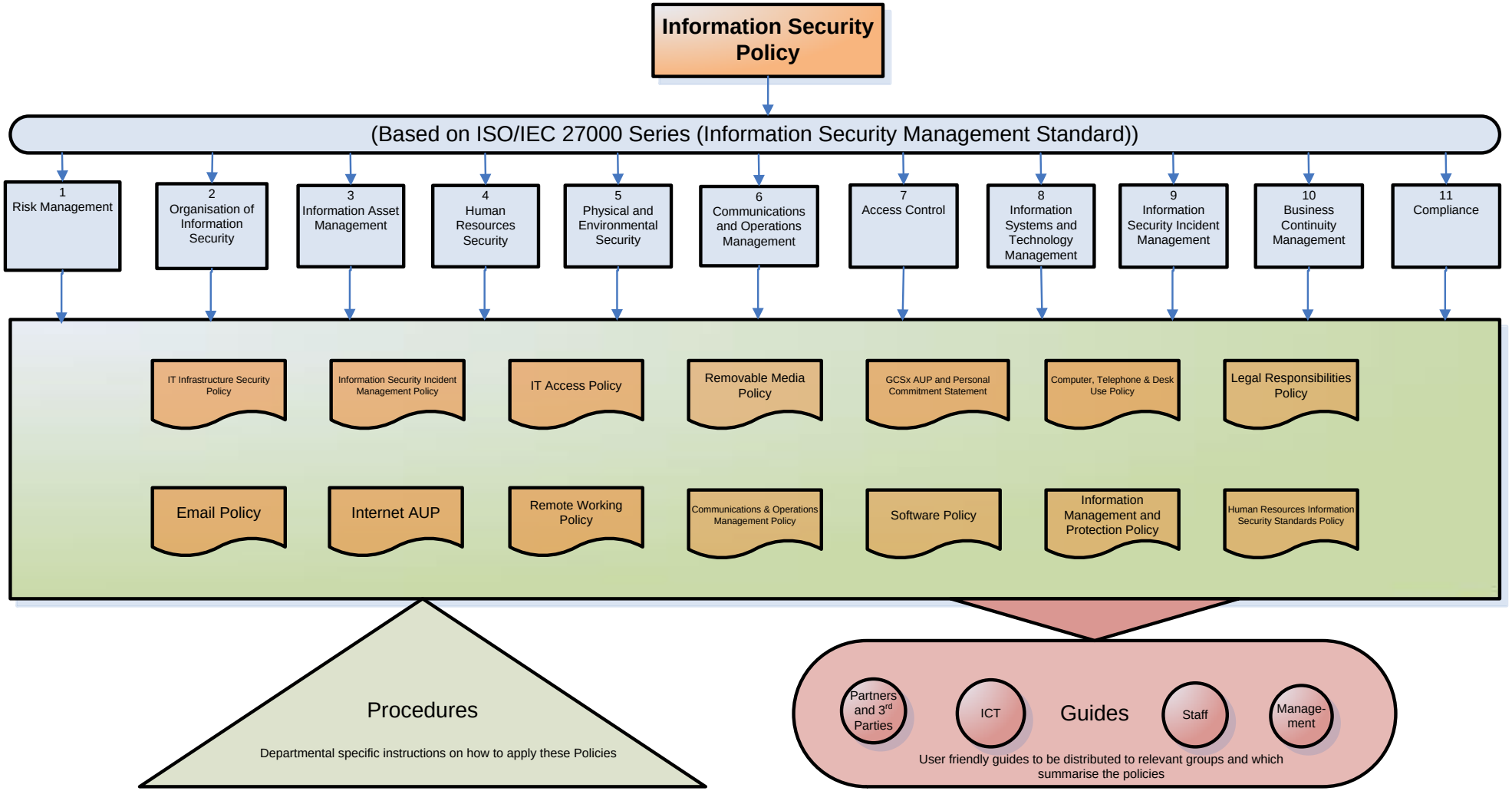
15.1 The design, operation, use and management of information systems must take into consideration all statutory, regulatory and contractual security requirements as well as organisational security policies and standards.

15.2 The security of information systems will be regularly reviewed and audited in order to ensure that they comply with security policies and standards.

15.3 The Information Security Framework must provide the necessary controls to maintain compliance with the following codes and standards:

- Public Services Network (PSN) Code of Connection.
- Payment Card Industry Data Security Standard (PCI DSS).

Appendix 1 – Information Security Policy Framework



West Lindsey District Council

If you would like a copy of this leaflet in large clear print, audio, Braille or in another language, please telephone
01427 676676

Guildhall, Marshall's Yard
Gainsborough
Lincolnshire DN21 2NA
Tel: 01427 676676
Fax: 01427 675170

www.west-lindsey.gov.uk