

# Corporate Information Security Policy

---

Name: Corporate Information Security Policy

Version: 1.4

Issue Date: 20/10/2009



File	Corporate Information Security Policy	Page	1	Version	1.4
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

# Document Control

This is a CONTROLLED document and updates or changes to this document are authorized and then advised by email to the relevant document holders.

It is UNCONTROLLED when printed. You should verify that you have the most current issue.

## DOCUMENT HISTORY

## Author(s)

Names	Role
John Pritchard	ICT Enterprise Architecture Manager

## Document Log

---

Version	Status	Date Issued	Description of Change	Pages affected	Review
1.0		08/07/2003	Approved and adopted by the Chief Executive Management Team (CXMT).	All	
1.1	Final	11/10/2007	Review & updated	All	October 2008
1.2	Final	18/12/2008	Updates to reflect new organisational structure	All	October 2009
1.3	Final	20/10/2009	Removed ISO9001 logo	1	April 2011
1.4	Final	15/06/2011	Reviewed	All	June 2012

File	Corporate Information Security Policy	Page	2	Version	1.4
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

# Contents

1. Introduction .....	4
2. Importance of Security .....	4
3. Objectives .....	6
4. Scope .....	6
5. Information Security Management .....	6
6. Principles .....	6
7. Standards .....	7
8. Legal Compliance .....	7
9. Implementation .....	7
10. Individual Responsibilities .....	8
11. Supporting Documentation .....	8
12. Modification .....	8

File	Corporate Information Security Policy	Page	3	Version	1.4
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

## 1. Introduction

Continuous improvement in the cost and performance of computer technology and telecommunications provides numerous new opportunities for Herefordshire Council to utilise and exploit information assets in the management and provision of services to the community. Current technical developments seek to emulate natural human networking, permitting the exchange of information and ideas, incorporation of formal and informal processes in the workflow and access to large volumes and variety of information sources.

Whilst the aim is to provide facilities for employees to use freely in pursuit of their job there are, however, management and legal issues, which should be borne in mind to ensure the effective and appropriate use of information technology.

Information is an asset that, like other important business assets, has value to an organisation and consequently needs to be suitably protected. Information security protects information from a wide range of threats in order to ensure business continuity, minimise business damage and maximise return on investments and business opportunities.

## 2. Importance of Security

Herefordshire Council has a significant investment in computer systems and networks. In common with other organisations, to a large and continually increasing extent the Council is dependent upon the data, which is stored and processed, on its computers and the management information that is generated from the data.

The loss of data and computer processing facilities or breaches of data access security could incur significant costs, loss of revenue and damage to the Councils reputation as a result of:

- Business activities being fully or partially suspended.
- Having to restore the data, computer programmes and/or equipment.
- Unauthorised disclosure of confidential information relating to individuals and/or other confidential business information being made available to 'interested parties'.
- Fraudulent manipulation of cash or goods.

The preservation of the confidentiality, integrity and availability of information held not only electronically within systems but also on paper, microfiche, floppy discs or CD-ROM or any external storage device is therefore essential to the Council.

File	Corporate Information Security Policy	Page	4	Version	1.4
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

## Policy Statement

The objectives of information security are to ensure business continuity and minimise business damage by preventing and minimising the impact of security incidents. In deploying the Herefordshire County Council Information Security Management System ("ISMS"), the Board of Directors aim to reduce risks to an acceptable level.

### Policy

The purpose of the Policy is to protect the organisation's **Information Assets**<sup>(1)</sup> from all threats, whether internal or external, deliberate or accidental.

It is the Policy of the organisation to ensure that:

- Information will be protected against unauthorised access.
- Confidentiality of information will be assured<sup>(2)</sup>.
- Integrity of information will be maintained<sup>(3)</sup>.
- Regulatory and legislative requirements will be met<sup>(4)</sup>.
- Business Continuity plans will be produced, maintained and tested<sup>(5)</sup>.
- Information security training will be available to all staff.
- All breaches of information security, actual or suspected, will be reported to, and investigated by the Information Security Engineer.

### Implementation

- Procedures exist to support the policy. These include virus control, passwords and business continuity.
- Business requirements for the availability of information and information systems will be met.
- The Information Security Manager has direct responsibility for maintaining the Policy and providing advice and guidance on its implementation
- All managers are directly responsible for implementing the Policy within their business areas, and for adherence by their staff.
- It is the responsibility of each member of staff to adhere to the Policy.

Joint Chief Executive Officer:

**Chris Bull**

Head of ICT:

**Zack Pandor**

- (1) Information takes many forms and includes data stored on computers, transmitted across networks, printed out or written on paper, sent by fax, stored on tapes and diskettes, or spoken in conversation and over the telephone.
- (2) The protection of valuable or sensitive information from unauthorised disclosure or intelligent interruption.
- (3) Safeguarding the accuracy and completeness of information by protecting against unauthorised modification.
- (4) This applies to record keeping and most controls will already be in place; it includes the requirements of legislation such as the Computer Misuse Act and the Data Protection Act.
- (5) This will ensure that information and vital services are available to users when and where they need them.

File	Corporate Information Security Policy	Page	5	Version	1.4
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

### 3. Objectives

The objectives of this Corporate Information Security Policy are to protect the Council's information through clear direction and guidance to ensure that:

- The public and all users of the Council's systems are confident of the accuracy and integrity of the information used and produced.
- Business damage and interruption caused by security incidents are minimised.
- Confidentiality of personal and other sensitive information is assured.
- All legislative and regulatory requirements are met.
- The Council's Information Technology is used responsibly, securely and with integrity at all times.

### 4. Scope

All users granted access to the Councils information, computer facilities and their associated information networks.

### 5. Information Security Management

This Information Security Policy is issued with the approval and support of the **Chief Executive and Information Policy Group**.

The **Information Security Manager** has been empowered to act on behalf of the **Corporate Management Board** and has been delegated direct responsibility for ensuring adherence to Policy for adherence by **all** Council staff, elected members, contractors and partners using our systems.

### 6. Principles

The principles of Information Security applied by Herefordshire Council are:

- System access control.
- Communications and operations management.
- Systems development and maintenance.
- Personnel security.
- Physical and environmental security.
- Asset classification.
- Business continuity planning.
- Compliance with legislation.

File	Corporate Information Security Policy	Page	6	Version	1.4
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

## 7. Standards

The security of the Council's information can be achieved by implementing a suitable set of controls, which comply with the **International standard ISO27001** in the form of:

- Procedures.
- Organisational structures.
- Software functions.

## 8. Legal Compliance

Some aspects of the Council's security will be governed by statutory legislation including:

- The Freedom of Information Act 2000.
- The Human Rights Act 2000.
- The Electronic Communications Act 2000.
- Regulation of Investigatory Powers Act 2000.
- The Data Protection Act 1998.
- The Copyright Designs and Patents Act 1998.
- The Computer Misuse Act 1990.

## 9. Implementation

The **Information Policy Group (IPG)** has been appointed to approve Policy and monitor Information Security.

**Client Account Managers** have been appointed to ensure Directorate compliance with Policy within each Service.

The **Head of ICT Corporate and Customer Services** is responsible for ensuring that networks and communications, the operating systems and support software and computer centres are secure and meet Policy requirements.

**Internal Audit** will evaluate security controls while undertaking audit reviews in addition to undertaking specific Information Security audits on a regular basis.

All breaches of Information Security, actual or suspected will be reported and investigated by the **Information Security Section**.

The **Information Security Manager** is responsible for delivery of an Action Plan to achieve accreditation to ISO270001

Compliance with Policy will require the keeping of records of policies, procedures and security reports. The Council's **Data Protection Officer (DPO)** supported by the **Data Protection Liaison Officers (DPLOs)** is responsible for producing and implementing an Archive and Data Retrieval Policy.

File	Corporate Information Security Policy	Page	7	Version	1.4
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

## 10. Individual Responsibilities

All Elected members must accept responsibility for maintaining Information Security standards within the organisation.

All managers<sup>1</sup> must accept responsibility for initiating, implementing and maintaining security standards within the organisation.

All non-managerial employees must accept responsibility for maintaining standards by conforming to those controls, which are applicable to them.

All ICT hardware or software that is intended to be used by employees of this authority must be procured through central ICT procurement.

Managers must undertake yearly assessments of security risks within their own areas to ensure that the cost of implementation of controls is proportionate to both the value of the information and the business harm likely to result from any security breach whilst complying with the controls of ISO270001.

## 11. Supporting Documentation

This Policy must be read in conjunction with any specific instructions issued for each information facility, and the following supporting documentation:

- **Internet Usage Policy**
- **E-mail Usage Policy**
- **Information Security Procedures**

## 12. Modification

The Council reserves the right to modify this Policy having given all users reasonable notice.

---

<sup>1</sup> A manager as defined in this policy is anyone who has responsibility for managing employees although the word manager may not appear in their job title.

File	Corporate Information Security Policy	Page	8	Version	1.4
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified