Herefordshire Council

Reference number	
Approved by	**IG Steering Group**
Date approved	**10 May 2018**
Version	**1.4**
Last Revised	
Review date	**May 2021**
Category	**Information Assurance**
Owner	**Information Governance Manager**
Who should read this	**All employees of Herefordshire Council**

INFORMATION SECURITY POLICY

After the Review Date has expired, this document may not be up-to-date. Please contact the document owner to check the status after the Review Date shown above.

If you would like help to understand this document, or would like it in another format or language, please contact the document owner.

Contents

1. Policy Statement

Information is one of the Council's most valuable assets. Preserving the confidentiality, integrity and availability of the information in our care is essential to maintain our position as a respected and trusted organisation. Herefordshire Council holds structured and unstructured information electronically in IT Systems and physically in paper records which must all be suitably protected. Information is at risk from a varied range of risks including: loss, unauthorised disclosure, fraud, vandalism, fire, flood, computer viruses, computer-hacking, social engineering and denial of service attacks.

The application of information security can protect information from these risks and aims to preserve:

- **Confidentiality**: ensuring 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

The Council is committed to protecting the confidentiality, integrity and availability of its information assets. The potential impact or damage to information assets is managed through the implementation of controls that balance risk against the cost of reduction or prevention.

2. Purpose

This security policy confirms the Councils commitment to the continuous improvement of Information Security and highlights the key areas and controls in place to effectively secure information in our care.

3. Scope

This policy applies to all staff, councillors, contractors and partners. All users have a role to play and a contribution to make to the safe and secure use of information and the technology used to manage it.

4. Definition

This policy is the minimum standard which should be applied whenever employee's access Council facilities and equipment.

In addition, local procedures, standards and work instructions may be defined to allow flexibility of organisational practices.

For the purposes of this policy ‘employee’ includes councillors, contractors and partners.

5. Management Responsibilities and Commitment

The Council’s IM&T Board and Information Governance Steering Group are committed to ensuring that all these aspects of information security are complied with to fulfil its statutory functions; to satisfy all applicable requirements within this policy. This information security policy has been established so that:

- It confirms the Council’s commitment to continuous improvement
- Highlights the key areas to effectively secure its information
- It is appropriate to the purpose of the organisation
- It provides the framework for setting continual information security objectives

This information security policy shall be available as documented information; be communicated within the organisation; and be available to interested parties, as appropriate. Compliance with this policy and all other security policies and procedures is mandatory for all staff.

The Information Governance Steering Group has the responsibility for ensuring that the policy is implemented and adhered to across the organisation.

6. Organisation of Information Security

The importance attached to information security is demonstrated by the existence of the Information Governance Steering Group. The Steering Group ensure that

- Security issues are reviewed and progressed
- Asses and approve Security risk assessments associated with changes to existing systems and the implementation of new systems.
- Monitoring the effectiveness of the information security (e.g. from the results of Internal and Third Party Audit reports and Security Incident Reports)
- Recommending /endorsing changes to information security

The Information Governance Steering Group meet monthly.

7. Human Resource Security

All employees must work in accordance with all policies and procedures which includes information security specific requirements. Furthermore a personal information security required to follow best practices regarding information security. There is also a procedure implemented for all employees that leave the Council (including temporary and contract employees) to disable their network account and recover all items of property.

All new employees (permanent and temporary) must complete the Information Security mandatory training module before being provided with access to the network. The module must also be completed on an annual basis as a refresher

Council information must be classified according to its sensitivity and an information owner assigned.

8. Access Control

Employees and contractors must be aware of and must follow a number of controls and procedures, which exist to limit access to confidential information. The Information Governance Manager is responsible for both establishing and maintaining robust logical access controls. An access control policy is in place and must be complied with by all employees and third parties.

9. Physical and Environmental Security

Employees must be aware of and must follow the detailed set of measures, controls and procedures that exist to ensure adequate control of physical security. These include:

- Building and individual alarm systems
- Restricted access to the building and further restricted access within it
- Secure lockers, drawers, storage and safes
- Clear desk and clear screen policy

10. Operations Security

Hoople Technology and Transformation will ensure correct and secure operations of information processing facilities.

11. Communications Security

Employees must be aware that the use of technology and communications are established, controlled and managed by the Information Governance Steering Group. They are responsible for ensuring that the appropriate security measures and processes are in place. Hoople Technology and Transformation will ensure that secure network, mobile and remote working measures are adequately protected.

12. System Acquisition, Development and Maintenance.

Appropriate information security processes must be included within all procurement activities and projects. Information security requirements for mitigating the risks associated with supplier's access to the organisation's assets must be agreed with the supplier and documented

13. Information Security Incident Management.

Security incident records must be centrally maintained, updated and monitored via a manual process. All employees must be aware of what constitutes an actual or potential security incident, how to report the incident and who to report the incident to.

The responsibility for the oversight of incidents rests with the Information Governance Manager.

14. Compliance

The Council must avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

The Council must take technical and organisational measures to protect personal data against accidental or unlawful destruction, or accidental loss or alteration and unauthorised disclosure or access. In particular the Council takes measures that are intended to ensure that:

- Anyone managing and handling personal data understands that they are contractually responsible for following good data protection practice

- Everyone managing and handling personal data is appropriately trained to do so

- Everyone managing and handling personal data is appropriately Supervised

15. Policy Compliance

If any user is found to have breached this policy, they may be subject to disciplinary action. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager.

Anyone suspecting that there has been, or is likely to be a breach of information security, is asked to inform their Line Manager or Team Leader immediately.

16. Review

This policy will be reviewed as it is deemed appropriate, but at least every 3 years

Version Log

Version	Status	Date Issued	Description of Change	Pages affected	Review
0.1	Draft		Approval to use of WM template obtained from KI Steering Group 12/02/2013	All	
1.0	Issued	30/04/2013	Approved by IM&T Board	All	March 2014
1.1	Issued	22/04/2015	ISO27001 Logo Removed and Policy Reviewed	All	March 2015
1.2	Issued	12/11/2014	Updated to reflect changes to the government protective marking scheme	All	November 2015
1.3	Draft		Updated to reflect IG Policy Set changes	All	
1.3	Final	14/01/2016			January 2019
1.4	Issued	14/05/2018	Updated to align with Hoople Policy and GDPR	All	May 2021