NHS
Herefordshire and Worcestershire
Clinical Commissioning Group

Corporate Information Security Policy

Information Security Policy

Document Reference Information

Version:	1.0
Status:	Ratified
Author:	Alicia Dunsby
Directorate responsible:	Digital
Directorate lead:	Director of Digital Strategy and Infrastructure
Ratified by:	Clinical Executive Commissioning Commitee
Date ratified:	1st July 2020
Date effective:	1st July 2020
Date of next formal review:	3 years from effective date
Target audience:	All permanent and temporary employees of the CCG, Governing Body members, contractors, agency staff.

Version Control Record

Version	Description of change(s)	Reason for change	Author	Date
0.1	First draft	First draft	Alicia Dunsby	01/02/2020
1.0	Final for sign off	Reviews by Lynda Williams, Alicia Dunsby and Tony Cirello	Alicia Dunsby	30/04/2020

Contents

1. Policy Statement ____ 3
2. Purpose ____ 3
3. Scope ____ 3
4. Definition ____ 3
5. Executive Leadership Responsibilities and Commitment ____ 4
6. Organisation of Information Security ____ 5
7. Human Resource Security ____ 5
8. Physical and Environmental Security ____ 6
9. Operations Security ____ 6
10. Communications Security ____ 6
11. System Acquisition, Development and Maintenance ____ 6
12. Supplier Relationships ____ 6
13. Information Security Incident Management ____ 6
14. Information Security Aspects of Business Continuity Management ____ 7
15. Compliance ____ 7
16. Equality Statement and Due Regard ____ 8
17. Linked Documents and Policies ____ 8

Policy Statement

Information is one of Herefordshire and Worcestershire CCG'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 and Worcestershire CCG 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

Herefordshire and Worcestershire CCG 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.

Purpose

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

Scope

This policy applies to all permanent and temporary employees of Herefordshire and Worcestershire CCG, contractual third parties and agents of Herefordshire and Worcestershire CCG with access to Herefordshire and Worcestershire CCG's information assets whether these be physical or electronic. 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.

Definition

This policy is the minimum standard which should be applied whenever employees access Herefordshire and Worcestershire CCG data, facilities and equipment, and

especially when managing, developing, configuring or maintaining information technology facilities and equipment.

In addition, local procedures, standards and work instructions may be defined to allow flexibility of organisational practices. This policy provides a minimum requirement to be met under nationally recognised standards.

For the purposes of this policy 'employee' includes contractors and agents.

Executive Leadership Responsibilities and Commitment

Herefordshire and Worcestershire CCG's Executive Leadership Team is 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 and to the continual improvement of Information Security. This information security policy has been established so that it:

- confirms Herefordshire and Worcestershire CCG's commitment to continuous improvement
- highlights the key areas to effectively secure its information
- is appropriate to the purpose of the organisation
- 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 Clinical Executive and Commissioning Committee (CECC) approves this policy.

The Executive Leadership team has the responsibility for ensuring that the policy is implemented and adhered to across the organisation.

Executive management will continue to demonstrate leadership and commitment with respect to Information Security by:

- Ensuring the information security policy and associated policies and guidance are established and are compatible with the strategic business direction of the organisation
- Ensuring the integration of the Information security requirements into the organisation's processes
- Ensuring that the resources needed for the management of information security are available to the organisation
- Communicating the importance of effective information security management and of conforming to the information security requirements

- Ensuring that the information security arrangements achieve intended outcome(s)
- Directing and supporting persons to contribute to the effectiveness of information security management
- Promoting continual improvement; and supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

Organisation of Information Security

The importance attached to information security is demonstrated by the existence of the Corporate IT Group and the Corporate Information Governance Group. The function of these Groups in relation to information security is outlined below:

- Reviewing and progressing strategic security issues
- Establishing relationships outside of Herefordshire and Worcestershire CCG with other security advisers
- Assessing the impact of new statutory or regulatory requirements imposed on Herefordshire and Worcestershire CCG
- Monitoring the effectiveness of the Information Security policies and arrangement (e.g. from the results of Internal and Third Party Audit reports and Security Incident Reports)
- Recommending /endorsing changes to the information security arrangements
- Reviewing and updating this policy.

These Groups meet regularly to address the above activities in order to assure the continuing effectiveness of Herefordshire and Worcestershire CCG's Information security policies and processes.

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 (acceptable use) policy ensures that employees are made aware that they are required to follow best practices regarding information security. There is also a procedure implemented for all employees that leave Herefordshire and Worcestershire CCG (including temporary and contract employees) to disable their network account and recover all items of property.

All new employees (permanent and temporary) must be trained on procedures in the areas described above as part of their induction programme. Ongoing training is provided via the mandatory training required by the organisation.

Herefordshire and Worcestershire CCG's information must be classified according to its sensitivity and an information owner assigned. The Information Asset Owners will

maintain an information asset inventory which is updated periodically, according to its risk profile and protected accordingly.

[redacted]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, safes and fireproof storage for physical backup media
- Secure offsite backups and archiving
- Clear desk and clear screen policy
- Procedures for the issue of removable media (USB's and laptops).

[redacted]Operations Security

Herefordshire and Worcestershire CCG will ensure correct and secure operations of information processing facilities.

[redacted]Communications Security

Employees must be aware that the use of technology and communications are established, controlled and managed by the Senior Information Risk Owner (SIRO). They are responsible for ensuring that the appropriate security measures and processes are in place. Herefordshire and Worcestershire CCG will ensure that secure network, mobile and remote working measures are adequately protected.

[redacted]System Acquisition, Development and Maintenance

All Herefordshire and Worcestershire CCG executive directors must ensure that appropriate information security processes are included in all projects.

[redacted]Supplier Relationships

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.

[redacted]Information Security Incident Management

Security incident management 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. Employees should refer to the IG Handbook section on Data Security and Protection Incidents for details of the procedures to be followed.

The responsibility for the oversight of breaches of technical and physical security rests with the SIRO.

[redacted]Information Security Aspects of Business Continuity Management

Herefordshire and Worcestershire CCG must ensure a consistent and effective approach to the management of major information security incidents, including communication on security events and weaknesses and the implications for business continuity management.

[redacted]Compliance

Herefordshire and Worcestershire CCG must avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

Herefordshire and Worcestershire CCG 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 Herefordshire and Worcestershire CCG 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.

Policy Compliance

Herefordshire and Worcestershire CCG is committed to effective Information Security Management.

If any user is found to have breached this policy, they may be subject to Herefordshire and Worcestershire CCG's disciplinary procedure. 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.

[redacted]Equality Statement and Due Regard

The CCG aims to design and implement policy documents that meet the diverse needs of our services, population and workforce, ensuring that none are placed at a disadvantage over others. It takes into account current UK legislative requirements, including the Equality Act 2010 and the Human Rights Act 1998, and promotes equal opportunities for all. This document has been designed to ensure that no-one receives less favourable treatment due to their personal circumstances, i.e. the protected characteristics of their age, disability, sex, gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity. Appropriate consideration has also been given to gender identity, socio-economic status, immigration status and the principles of the Human Rights Act.

In carrying out its functions, the CCG must have due regard to the Public Sector Equality Duty (PSED). This applies to all the activities for which the CCG is responsible, including policy development, review and implementation.

[redacted]Linked Documents and Policies

Personal Information Security Responsibilities

Information Governance Management Framework

Information Governance/Data Security and Protection Policies

Information Governance Handbook

Staff Code of Conduct