NHS
Coventry and Warwickshire
Integrated Care Board

Information Security Policy

Reference Number:	This will be applied to all new ICB-wide PPSs by the Governance and Corporate Affairs Team and will be retained throughout its life span.
Version:	Version 1.0
Name of responsible Committee and date approved or recommended to Integrated Care Board Board:	Audit Committee
Date approved by the Integrated Care Board (if applicable):	1 July 2022
Next Review Date:	1 April 2024
Expiry Date:	1 October 2024
Name of author and title:	Laura Collett, IT Security Lead, ICB
Name of reviewer and title:	Phil Johns, Chief Executive, ICB
Department:	Corporate Office

VERSION HISTORY

Date	Version	Changes made to previous version	Consulting and Endorsing Stakeholders, Committees / Meetings / Forums etc.

Contents

1. Introduction....4
2. Purpose....4
3. Definitions....4
4. Roles and Responsibilities....5
5. Process....6
6. Training....9
7. Monitoring Compliance and Effectiveness of the Policy....9
8. References and Further Reading....10
Appendix A - Equality Impact Assessment....11

1. Introduction

1.1. Information is one of NHS Coventry and Warwickshire Integrated Care Board's ("the ICB") most important assets. The ICB and its staff have responsibilities and legal requirements to keep information safe, secure and confidential at all times. Particular care must be taken with both patient and staff personal confidential data.

1.2. The ICB will comply with all relevant legislation, this includes:

- The Data Protection Act 2018;
- The Human Rights Act 1998;
- The Computer Misuse Act 1990;
- The Copyright Designs & Patents Act 1988;
- The Freedom of Information Act 2000;
- The Regulation of Investigatory Powers Act 2000;
- Data Retention and Investigatory Powers Act 2014.

1.3. The ICB is also required to comply with the NHS Information Governance Assurance Statement and the requirements in order to link to the national N3 network.

1.4. This policy provides a high-level overview of the ICB's commitment to ensure effective information security management. It must be read in conjunction with the ICB's:

- Email Usage Policy;
- Internet Usage Policy;
- Removable Media Policy;
- Safe Haven Policy;
- Incident Reporting Policy.

2. Purpose

2.1. The aim of this policy is to establish and maintain the security and confidentiality of information, information systems, applications, and networks owned or held by the ICB and the provider of Corporate IT services (the 'provider').

3. Definitions

3.1. **HSCN – Health and Social Care Network/Trust Network**

The national secure NHS network to which provider owned Computer/Laptops are connected.

3.2. **Server**

The provider's server runs the administrative software that controls access the network and its resources.

3.3. **Firewall**

A device that blocks unauthorised access to an organisation's local area network (LAN). The firewall sits on the server acts as the LAN's gateway to the internet, or it can be a dedicated computer placed between the LAN and the Internet, so that the network is never in direct contact with the Internet.

The firewall also keeps track of every file entering or leaving the local area network in order to detect the sources of viruses and other problems that might enter the network.

3.4. **Asset(s)**

Any information system, computer or Information Technology (IT) equipment or programme owned by the ICB and the provider and which stores data.

3.5. **Encryption**

Encryption is a way to enhance the security of a file by scrambling the contents so that it can be read only by someone who has the right password to unscramble it. Encryption software turns text into code format, therefore undecipherable.

Encryption software must be provided by the provider's IT Department. Individual's own software is not accepted by the ICB and the provider and may not meet the Department of Health's specifications.

3.6. **Software**

This refers to computer programmes which are sometimes also called applications.

3.7. **Virus**

An unauthorised piece of computer code attached to a computer programme which secretly copies itself using shared discs or network connections. Viruses can destroy information or make a computer inoperable.

3.8. **Cyber Security**

Cyber Security is the protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide.

4. Roles and Responsibilities

4.1. The ICB's Chief Executive has ultimate accountability for information security within the ICB, ensuring systems and processes are in place to adequately meet its requirements.

4.2. The ICB's Chief Transformation Officer is responsible for ensuring:

- processes are in place for the safeguarding of information during storage and transfer;
- systems and equipment are in place to allow for the safeguarding of information on the provider's server and virus protection and encryption software is available.

4.3. The Senior Information Risk Owner (SIRO) role is performed by the ICB's Associate Director of Governance and Corporate Affairs. As SIRO they are responsible to the ICB's Governing Bodies and Accountable Officer for reporting information security risks.

4.4. The ICB's Caldicott Guardians are responsible for ensuring that the ICB is compliant with the confidentiality requirements of the Data Protection Act 2018.

4.5. The ICB's Information Governance Steering Group (IGSG) is responsible for the implementation of the Information Governance work programme. Compliance reports will be received and reviewed and where non-compliance is identified action will be agreed and monitored by the IGSG.

4.6. The ICB's Associate Director of Governance and Corporate Affairs is responsible for ensuring procedures are implemented to ensure the safeguarding of information. They advise the IGSG on non-compliance and provide advice and support to staff as required.

4.7. The Data Protection Officer (DPO) is responsible for informing and advising the organisation and its employees of their obligations pursuant to the General Data Protection Regulations (GDPR) and national data protection legislation, and monitoring compliance, reporting to the highest management level of the organisation – i.e. board level.

4.8. The provider's Information Technology (IT) Department is responsible for the day-to-day operational management of all technical security processes. This is overseen and reviewed by the provider's Information Security Manager who is a member of the provider's Information Governance Group and who is responsible for reporting to the provider's Information Governance Group in regard to IT risks.

The provider's IT Department is responsible for the implementation and management of technical controls which are designed to protect information held within the provider's IT environments.

The provider's IT Department is responsible for managing and maintaining the Asset Register and assigning Asset Owners for all provider assets.

4.9. Information Asset Owners/Information Asset Administrators are responsible for ensuring that information assets are secured against the threats to them to an appropriate degree.

4.10. Every staff member is responsible for ensuring they comply with this policy and all other associated policies and procedures.

Security requirements are addressed at the recruitment stage and contracts of employment contain a confidentiality clause.

Security requirements are included in job definitions where required.

All staff have a duty to report any actual or potential information security incidents in accordance with the ICB's Incident Reporting Policy.

5. Process

5.1. **Asset Register / Asset Owners**

Both the provider and the ICB must have up-to-date Asset Registers for the assets each owns.

The provider's IT Asset Registers must be maintained by its IT Department and reviewed annually. The Registers must include:

- Information assets: databases, data files, archived information;
- Software assets: system software, application software;

- Physical assets: computer equipment, technical equipment.

Every asset (hardware, software, application or data system) will have a named Asset Owner who will be responsible for the security of that asset.

The ICB's Asset Register(s) are maintained by the Corporate Governance Manager and the relevant Information Asset Owner and are reviewed annually: The Registers must include:

- Information assets: databases, data files, archived information;
- Software assets: system software, application software;
- Physical assets: computer equipment, technical equipment.

5.2. **Access Controls**

Only authorised personnel who have a justified and an approved business need can be given access to restricted areas i.e. information systems or stored data.

Access controls will be managed in adherence with the provider's System Level Security Protocol and, in relation to the ICB's network directories with the ICB's System Level Security Protocol.

5.3. **Remote Access**

Remote access can be made available to staff as appropriate, with manager approval. Remote Access must be made via the provider's IT Department procedures.

5.4. **Internet Connections**

Where the provider's equipment used by the ICB is connected to a network, connection to the internet is only permitted through the connection provided by the provider's IT Department.

The Internet must be used in adherence with the ICB's Internet Usage Policy.

5.5. **Password Management**

Staff will have passwords in order to access restricted areas i.e. information systems or stored data.

Staff must ensure passwords remain secure at all times and must not be shared with others.

All actions taken during staff log in will be monitored by the provider's IT Department and any inappropriate or misuse may result in disciplinary action.

5.6. **Email Access**

Staff must only use email accounts approved for use and assigned by the provider's IT Department.

Personal email accounts must not be used for business purposes.

Email must be used in adherence with the ICB's Email Usage Policy.

5.7. **Removable Media / Devices**

Staff must only use removable media / devices approved for use by the provider's IT. These will be managed by forcing encryption if plugged into the provider's computers linked to the Network.

Removable media/devices must be used in adherence with the ICB's Removable Media Policy.

Due to ICB staff having access to remote working, the use of removable media should only be required in a limited number of situations.

5.8. **Storing / Saving Information**

When saving information this must be done using the provider's computers / laptops connected to the server only or other agile devices that are linked to the provider's Network or have the ability to be uploaded to the provider's Network.

Information must not be stored to home drives or personal equipment. Provider supported equipment is secure and also enables regular back-ups to be taken by the provider's IT to ensure loss of data is kept to a minimum during service disruption.

Information must never be stored on the desktop or C: drive – these areas are not backed-up to the provider's server and can be accessed by anyone using that machine/equipment.

5.9. **Physical and Environmental Security**

To maintain availability of services, critical provider IT equipment, such as servers and core networking equipment, will be protected against physical and environmental threats such as:

- Theft, vandalism, and accidental damage;
- Fire and flood damage;
- Overheating;
- Loss of power;
- Cyber-attacks.

The provider's IT Department will assess the risks to critical provider IT equipment and will provide the necessary facilities and resources to adequately mitigate the risks.

All PC's and servers under the control of the provider will be protected from electronic threats such as viruses.

5.10. **Firewalls**

The provider's IT Department will be required to configure the network to include firewalls to ensure, as far as is practical, separation of the provider's networks from other networks.

The provider's IT Department will be required to position firewalls to protect any particularly sensitive servers or other equipment from other parts of the network. For example, if it is not possible to load anti-virus software on a particular server, the traffic to and from that server should be protected by a firewall.

The provider's IT Department will be required to configure firewalls in such a way as to ensure that only the minimum required traffic is allowed through the firewall.

5.11. **Software**

Only licensed copies of approved commercial software will be installed on the provider's equipment. It is a criminal offence to make or use unauthorised software and users of such will face disciplinary action.

5.12. **Virus Protection**

All provider computers, laptops and servers will be protected with anti-virus software.

Staff must report any detected or suspected viruses to the provider's IT Department immediately.

5.13. **Information Security Incidents - including Cyber Security incidents**

A security incident is any of the following:

- Loss or theft of provider equipment;
- Loss or theft of data / information;
- Unauthorised access to information / systems;
- Threat to the security of the provider's Network either by introduction of viruses or other malware and or disruption to service provision.

All information security incidents must be reported immediately via the ICB's Incident Reporting Policy to the ICB's Corporate Governance Manager. The provider's Information Security Manager must also be informed.

5.14. **Business Continuity and Disaster Recovery**

The provider must ensure that business continuity and disaster recovery plans are maintained for all critical information, applications, systems and networks it provides to the ICB. These must be reviewed at least annually.

The ICB must ensure that business continuity and disaster recovery plans are maintained for all critical information, applications and systems it owns. These must be reviewed at least annually.

6. Training

6.1. The ICB will carry out an annual Training Needs Assessment (TNA) and staff are required to undertake relevant training, including mandatory Data Security Awareness training.

6.2. The TNA is monitored by the DPO, Senior Management Team and the Audit Committee.

6.3. Information Security is included in the Corporate Governance induction for all new employees of the ICB.

7. Monitoring Compliance and Effectiveness of the Policy

7.1. The Clinical Quality and Governance Committee will oversee implementation of the policy and will receive quarterly reports detailing incidents logged.

7.2. The Clinical Quality and Governance Committee reviews the mitigation of information security risks.

7.3. The SIRO will report information security risks, including Cyber Security threats, and breaches to the Governing Bodies.

7.4. Training data is regularly reviewed by the Clinical Quality and Governance Committee.

7.5. The policy will be reviewed every three years by the Governing Bodies.

8. References and Further Reading

8.1. Related references and further reading:

- The Data Protection Act 2018;
- The Human Rights Act 1998;
- The Computer Misuse Act 1990;
- The Copyright Designs & Patents Act 1988;
- The Freedom of Information Act 2000;
- The Regulation of Investigatory Powers Act 2000;
- Data Retention and Investigatory Powers Act 2014;
- The NHS Information Governance Assurance Statement;
- General Data Protection Regulations and the current national data protection legislation
- System Level Security Protocol.

Appendix A - Equality Impact Assessment

Policy	Information Security Policy	**Person completing EIA**	Laura Whiteley, Corporate Governance Manager Victoria Watts, Governance Officer
Date of EIA	06/03/19	**Accountable ICB Lead**	Anita Wilson, Associate Director of Governance and Corporate Affairs

Aim of Work	To set out the ICB's policy for information security, within the bounds of legal and professional obligations.
Who Affected	All staff and data subjects

Protected Group	Likely to be a differential impact?	Protected Group	Likely to be a differential impact?
Sex	No	**Age**	No
Race	No	**Gender Reassignment**	No
Disability	Yes	**Marriage and Civil Partnership**	No
Religion / belief	No	**Pregnancy and Maternity**	No
Sexual orientation	No		

Describe any potential or known adverse impacts or barriers for protected/vulnerable groups and what actions will be taken (if any) to mitigate. If there are no known adverse impacts, please explain.

To ensure that individuals with specific disabilities can access the policy and its content, the document will be made available in alternative formats if required.