**Appendix 2**

# Policy

ANGUS
Health & Social Care
Partnership

# Information Security

| | | | |
|---|---|---|---|
| **Version Number:** | **V0.3** | **Owner:** | Alison Clement |
| **Issue Date:** | 06/06/2019 | **Review Date:** | |

## Version History

| Version No. | Issue Date | Description | Author |
|---|---|---|---|
| 0.1 | 08/05/2019 | Initial Draft for Consultation | Keith Whitefield |
| 0.3 | 06/06/2019 | Final draft for approval | Keith Whitefield |
| | | | |
| | | | |
| | | | |
| | | | |

# Contents

# 1 Policy Statement

Information is a vital asset to AIJB and is an essential element to all aspects of its work. The AIJB recognises the need to ensure that information is processed in a secure manner and is appropriately protected from misuse, unauthorised or accidental modification, destruction, or disclosure.

Most of the functions of the AIJB are carried out on its behalf by NHS Tayside and Angus Council under the direction of the AIJB, or by third parties contracted by those bodies on the AIJB's behalf. The AIJB depends upon those organisations to implement and maintain robust technical and organisational measures to ensure the security of the AIJB's information assets at all times.

This policy sets out the principles and general standards which the AIJB expects to be maintained by all parties responsible for handling any information for which the AIJB is ultimately accountable.

This policy must be applied in a way which is consistent with the objectives of the AIJB's policies on Data Protection, Records Management, and Access to Information.

## 1.1 Scope

The Information Security Policy applies to:

- Any information assets for which the AIJB is ultimately accountable, solely or jointly with another party, whether created in the carrying out of the AIJB's functions or entrusted to it by a third party.
- The management and security of paper based records, information held on computer systems, data network communications, and information held on magnetic or optical media.
- Any organisation acting on behalf of the AIJB in carrying out the functions of the AIJB, including NHS Tayside and Angus Council.
- Any member of the AIJB, officer of the AIJB, or member of staff of any organisation holding or processing AIJB information assets, including NHS Tayside and Angus Council.
- Structured record systems (paper and electronic)
- Transmission of information (Fax, Email, post and telephone)

## 1.2 Definitions

For the purposes of this policy the following definitions are used:

**Information Asset** – information or data held in any form (e.g. paper, digital, audio, photograph, video) created by or on behalf of the AIJB, or for which the AIJB is solely or jointly accountable

**Information System** – any system or component of a system used to manage, process, or communicate AIJB information assets including digital networks, databases, software, hardware, etc. as well as physical filing and archive systems

**The Partners** – NHS Tayside and Angus Council

### 1.3 Principles

This policy reflects the AIJB's commitment to the following principles:

- **Confidentiality** – Access to information and to information systems shall be confined to those with appropriate authorisation.
- **Integrity** –Data and information shall be complete and accurate. All work systems, information systems, networks, and ICT equipment shall be secure and operate correctly, according to specification.
- **Availability** – Data and information shall be available whenever and wherever it is required.
- **Accountability** – Individuals shall be held accountable for any processing they carry out on information or data, including access, transfer, disclosure, sharing, alteration, or destruction.

## 2 Information Security Objectives

### 2.1 Access to information and Information Systems

The partners shall ensure that there are robust technical and organisational measures in place to ensure access to, and processing of, AIJB information assets is restricted to those persons authorised to access or process that information in the carrying out of the functions of the AIJB.

The partners shall ensure that access to, and use of, information systems used in the management, processing, or communication of AIJB information assets is restricted to those persons authorised to do.

The partners shall ensure that any third parties contracted by them to carry out functions of the AIJB have similar robust measures in place in respect of AIJB information assets and information systems used in relation to AIJB information assets.

### 2.2 Protection of Information Assets and Information Systems

The partners shall take all reasonable steps to ensure that AIJB information assets and the information systems used to manage, process, and communicate those information assets are protected from malicious attack, corruption, theft, or illegal use.

The partners shall ensure that any third parties contracted by them to carry out functions of the AIJB have similar robust measures in place in respect of AIJB information assets and information systems used in relation to AIJB information assets.

### 2.3 Encryption of Data and Data Communications

The partners shall take all reasonable steps to ensure that all electronic communication of AIJB information assets is encrypted during transmission, whether by email, file transfer, or any other means.

The partners shall ensure that secure email and/or file transfer capabilities are available for use in the communication of AIJB information assets with authorised third parties who do not have access to the secure Public Service Network (PSN).

Wherever practicable the partners shall implement measures to ensure AIJB information assets which exist in digital form are encrypted while at rest, especially where these contain personal data or are otherwise sensitive.

The partners shall ensure that any third parties contracted by them to carry out functions of the AIJB have similar robust measures in place in respect of AIJB information assets and information systems used in relation to AIJB information assets.

## 2.4 Storage and Transfer of Physical Information Assets

The partners shall implement robust measures to ensure that the storage and transfer of physical files or other media containing AIJB information assets is as secure and safe from loss or damage as possible.

The partners shall ensure that any third parties contracted by them to carry out functions of the AIJB have similar robust measures in place in respect of physical media containing AIJB information assets.

## 2.5 Monitoring and Accountability

The partners shall implement robust monitoring of any activity in relation to AIJB information assets including who has accessed, processed, amended, communicated, or disposed of any such asset. The partners shall ensure that records of such activity are available for audit for three years from the event to which the record relates.

## 2.6 Integrity and Version Control

As far as is practicable the partners shall ensure that all copies of AIJB information assets held by or processed by them, or by third parties on their behalf, are kept up to date and their integrity maintained, including ensuring that a locked current master copy of any AIJB information asset is separately retained.

## 2.7 Business Continuity

The partners shall implement business continuity plans and measures to ensure that AIJB information assets remain available at all times in the event of information system failure or any other cause.

## 2.8 Information Asset Registers and Designated Owners

The AIJB, in collaboration with the partners, shall compile and maintain a register of all its information assets, whether held by the AIJB or by any other person or organisation on its behalf.

The partners shall ensure that each asset identified on the register has a senior officer or service manager designated as the owner of that asset who will have responsibility for defining the appropriate uses of the asset and

ensuring that appropriate security measures are in place to protect the asset.

# 3 Roles and Responsibilities

## 3.1 Corporate Accountability

The AIJB is ultimately accountable for the security of its information assets.

NHS Tayside and Angus Council are accountable to the AIJB for:

- the secure handling of the AIJB's information assets in the carrying out of AIJB functions under the direction of the AIJB
- the security of the physical and digital systems, devices, and networks used in the processing of those assets as part of their carrying out of functions of the AIJB under the direction of the AIJB

## 3.2 AIJB Senior Information Risk Owner (SIRO)

The SIRO has overall strategic responsibility for governance in relation to data security risks. The AIJB's SIRO is the Clinical Director. The SIRO:

- Acts as advocate for information security as a member of the AIJB and the Executive Management Team.
- Liaises with the SIRO of NHS Tayside and Angus Council's Chief Information Governance Officer (CIGO) to secure the necessary assurances from both organisations regarding information security matters affecting the AIJB's information assets.

## 3.3 NHS Tayside SIRO

The person designated by NHS Tayside as senior information risk owner shall be accountable to the AIJB for information security in respect of the information assets of the AIJB created or processed by NHS Tayside in carrying out functions of the AIJB under the direction of the AIJB. They shall also be accountable to the AIJB for the security of information systems used by NHS Tayside to process AIJB information assets and compliance by NHS Tayside staff with NHS Tayside's information security policies. They shall also be accountable to the AIJB for the compliance with NHS Tayside's information security policies by any third party contracted by NHS Tayside to carry out functions of the AIJB on its behalf.

## 3.4 Angus Council CIGO

The person designated by Angus Council as chief information governance officer shall be accountable to the AIJB for information security in respect of the information assets of the AIJB created or processed by Angus Council in carrying out functions of the AIJB under the direction of the AIJB. They shall also be accountable to the AIJB for the security of information systems used by Angus Council to process AIJB information assets and compliance by Angus Council staff with the council's information security policies. They shall also be accountable to the AIJB for the compliance with the council's information security policies by any third party contracted by Angus Council to carry out functions of the AIJB on its behalf.

### 3.5 Information Asset Owners (IAO)

Senior managers of any service provided or commissioned by the AIJB, or provided or commissioned on its behalf by NHS Tayside or Angus Council in the carrying out of a function of the AIJB under the direction of the AIJB, are information asset owners in respect of AIJB information assets created or processed within their service area, and are responsible for ensuring information security in respect of those assets and the use of systems and networks

### 3.6 Individual Members of the Board, Members of Staff, and Volunteers

Individual members of the AIJB, and all staff and volunteers involved in carrying out any function on behalf of the AIJB, are responsible for the security of AIJB information assets created, held, or processed by them or which come within their care, and must comply with this policy and any guidance issued under this policy.

Where an individual is employed by or acting for Angus Council or NHS Tayside, or any third party commissioned by them, and is carrying out a function of the AIJB, they shall comply with any policy or guidance on information security issued by their employer so far as it does not conflict with the requirements of the AIJB information security policy or any guidance issued under it.

## 4 Governance

The Clinical, Care, and Professional Governance Forum (CCPG) is accountable to AIJB and the Executive Management Team through the SIRO, and is responsible for providing assurance to the AIJB and Executive Management Team in respect of all information governance matters including information security.

This includes:

- Reviewing data protection policies and guidance
- Raising awareness of best practice in information security
- Identifying and monitoring information risk
- Monitoring the management of adverse events including information security breaches and personal data breaches

## 5 Monitoring and Review

Compliance with this policy shall be monitored by the CCPG.

This policy will be reviewed annually by the CCPG and any revisions submitted to the AIJB for approval.

## 6 Related Policies and Procedures

- AIJB Data Protection Policy

- AIJB Records Management Policy
- AIJB Access to Information Policy
- Tripartite Information Governance Protocol