Appendix 3

Policy

ANGUS
Health & Social Care
Partnership

Protection of Personal Data

Version Number:	**0.3**	**Owner:**	Alison Clement, Clinical Director
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

To operate efficiently and effectively, Angus Integration Joint Board (AIJB) must collect and use information about people with whom it works. These may include current, past and prospective employees, volunteers, service users, and suppliers, and members of the general public.

The AIJB regards respect for the privacy of individuals and the lawful and careful treatment of personal data as critical to maintaining trust between the AIJB and the people it serves. The AIJB will ensure that it treats personal data lawfully and proportionately.

The AIJB is committed to protecting the rights and privacy of individuals including those rights set out in the General Data Protection Regulation (GDPR); the Data Protection Act 2018 (DPA), and other data protection legislation.

The AIJB's principal aim is to ensure that all personal data processing carried out by the AIJB, or on its behalf, complies with the six data protection principles and other key legislative requirements.

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

1.1 Scope

This policy applies to:

- The Angus Integration Joint Board corporately and it members individually
- Angus Council, NHS Tayside, and their respective employees in so far as they are engaged in carrying out AIJB functions under the direction of the AIJB
- Volunteers engaged in carrying out AIJB functions or providing services on behalf of the AIJB
- Independent contractors commissioned by the AIJB, or commissioned on its behalf by NHS Tayside or Angus Council, to carry out any AIJB function or provide services on behalf of the AIJB
- Any other individual or body performing a function of the AIJB on its behalf

1.2 Definitions

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

Personal Data (also referred to as Personal Information) – Data which relates to a living individual ("data subject") who can be identified:

- From the data; or
- From the data and other information which is in the possession of, or is likely to come into the possession of, the data controller.

This includes the data subject's name, address, telephone number, identification number (e.g. national insurance number), CHI number, IP

address, online contact details (e.g. email address) any record of their activity, relationships, details of services received by them, photographs, video, audio recordings, any expression of opinion about the individual, and any decision or indication of the intentions of the data controller or any other person in respect of the individual.

Special Category Data – Personal data consisting of information as to any of the following:

- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.
- Genetics.
- Biometrics where these can be used for ID purposes, including photographs and audio or video recordings.
- Health and social care.
- Sex life.
- Sexual orientation.

Special category personal data is subject to additional conditions of processing (see Appendix 2).

Personal Data Record – A record is recorded personal data, in any form, which is created, received or maintained by the AIJB or on its behalf in the carrying out of the AIJB's functions, in respect of which the AIJB is a data controller.

Information Asset (Personal Data) – A class or records containing personal data held by or on behalf of the AIJB in respect of which the AIJB is a data controller.

Format – A record can be in any format including (but not limited to) paper files, e-mail, audio/visual, electronic documents, systems data, databases, digital images and photographs.

Data Subject – A person whose personal data is processed by, or on behalf of, the AIJB.

Records Management – The control of the AIJB records during their lifetime, from creation to storage until archiving or destruction, whether those records are held by the AIJB or on its behalf.

Record Keeping System – A system or procedure by which the records of the AIJB are created, captured, secured, maintained and disposed.

Processing – Any activity in relation to the handling of personal data from obtaining and organising that information to using the information, sharing the information and storing that information, and destroying the information when it is no longer required.

Data Controller – A Data Controller is a person or organisation who decides how any personal data can be held and processed, and for what purposes. AIJB is a Data Controller.

Joint Data Controllers – Any persons or organisations (e.g. AIJB and NHS Tayside or Angus Council) who are jointly data controllers in respect of personal data about an individual or group of individuals.

Data Processor – Any person or organisation who processes personal data on behalf of the AIJB under the direction of the AIJB.

Purposes – The objectives for which personal data is being processed. These must be specific and have a legal basis within the terms of the data protection legislation.

Data Protection Legislation – All legislation which governs the processing of personal data by or on behalf of the AIJB, including, but not limited to:

- Human Rights Act 1998 (HRA)
- The Public Bodies (Joint Working) (Scotland) Act 2014 (Joint Working Act)
- General Data Protection Regulation 2016 (GDPR)
- Data Protection Act 2018 (DPA)

1.3 Principles

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

Confidentiality – the privacy, freedoms, and rights of the data subject are protected and information is not disclosed without legal basis or for illegitimate purposes

Integrity – information about a data subject is kept up to date, accurate, and as complete as possible

Availability – the information is available at all times for the purposes for which it is processed

Accountability – the data controller and processor are accountable to the data subject for their actions in processing the data subject's information and enable the data subject to exercise their rights over their information

2 General

2.1 Registration with the Information Commissioner

The AIJB is a data controller as defined in the data protection legislation in respect of all personal data processed by the AIJB, or by third parties on its behalf in the carrying out of the AIJB's functions.

The AIJB shall register as a data controller with the Information Commissioner, as required under the Data Protection (Charges and Information) Regulations 2018, and comply with any legal requirements arising from registration.

The AIJB registration number is **ZA404048**.

2.2 Appointment of Data Protection Officer

The AIJB shall appoint a data protection officer as required under Article 37(1)(a) of the GDPR.

2.3 Register of Information Assets (Personal Data)

The AIJB, in collaboration with NHS Tayside and Angus Council, shall compile and maintain a register of information assets containing personal data records for which it is a data controller, whether held by the AIJB or by any other person or organisation on its behalf.

3 Processing of Personal Data

3.1 Purposes of Processing

Personal data shall only be processed in order to support those functions the AIJB is legally entitled to carry out.

3.2 Legal Basis for Processing

Personal data shall only be processed where there is a legal basis for doing so under Article 6(1) of the GDPR, and special category data shall only be processed where one of the conditions set out in Article 9(2) of the GDPR is also met. (See Appendix 2)

In line with statutory guidance, "Explicit consent" will not be used as a legal basis for processing except where processing is for purposes other than the AIJB's core functions, e.g. marketing.

3.3 Privacy Notices

All data subjects shall be provided with a privacy notice.

Three levels of privacy notices will be available:

- A general privacy notice suitable for all service users
- Service specific privacy notices where the purposes of processing and data sharing arrangements differ from those set out in the general privacy notice
- A comprehensive privacy statement covering all personal data processing carried out by, or on behalf of, the AIJB

Privacy notices shall comply with the requirements of the GDPR. Where the AIJB is a joint data controller this will be reflected in the privacy notice.

All privacy notices shall be published on the AIJB website.

4 Sharing of Personal Data

On occasion personal data, in respect of which the AIJB is a data controller, may be shared with other organisations in pursuance of the AIJB's legal duties and functions. All data sharing must comply with the requirements of the data protection legislation and shall have due regard to the Data Sharing Code of Practice issued by the Information Commissioner.

The AIJB shall establish a data sharing framework with NHS Tayside and Angus Council under the provisions of section 49 of the Public Bodies (Joint Working) (Scotland) Act 2014 which shall govern the sharing of personal data between those bodies and by those bodies with any third party.

Personal data, in respect of which the AIJB is a data controller, shall not be shared on a regular, routine, or bulk basis with a third party unless an information sharing agreement (ISA) has been agreed with that third party.

The AIJB shall maintain a register of all current ISAs and will publish the ISAs in accordance with the AIJB Publication Scheme.

Only personal data necessary to the purpose of the data sharing shall be shared. Wherever possible personal information shall be pseudonymised to prevent identification of the data subject by third parties.

5 Compliance

5.1 Processing of Personal Data

In processing personal data, or requiring personal data to be processed on its behalf, the AIJB shall ensure compliance with the data protection legislation and have due regard to relevant codes of practice issued by the Information Commissioner.

5.2 Data Subject Access

The AIJB shall establish a formal agreement with NHS Tayside and Angus Council on the handling of requests by data subjects to exercise their right of access and other rights in respect of personal information for which the AIJB and one or both of the other bodies are joint data controllers.

The AIJB shall ensure that data subjects are able to exercise their rights under the data protection legislation including their right of access to their personal data.

Access by a data subject to their personal data shall only be refused under the circumstances defined in Parts 2 to 4 of Schedule 3 of the Data Protection Act 2018.

Due care will be taken in responding to data subject access request to ensure that the rights of any other third parties are protected through redaction of documentation where necessary.

In line with the AIJB's policy of openness, and in accordance with the provisions of Section 17 of Schedule 2 of the Data Protection Act 2018, the details of heath, social care, and education professional involved in the care and support of the data subject, shall not be redacted from any personal record which must be disclosed in response to a data subject's request to access their personal data.

5.3 Data Protection Impact Assessments (DPIA)

No new or revised process or service which involves the processing of personal information by, or on behalf of, the AIJB shall commence until a DPIA has been carried out and the AIJB's Senior Information Risk Owner is satisfied that sufficient measures have been taken to mitigate any potential risks to the rights and freedoms of data subjects.

All DPIAs shall be carried out using the AIJB's approved methodology and documentation.

5.4 Data Protection by Default and Design

All processing of personal data must be designed in such a way that there are sufficient, effecting technical and n compliance with Article 25 of the GDPR, all new services or procedures shall be designed from

5.5 Management of Personal Data Breaches

The AIJB shall establish a formal agreement with NHS Tayside and Angus Council on the handling of personal data breaches in respect of personal information for which the AIJB and one or both of the other bodies are joint data controllers.

Any incident which may be a personal data breach must be reported immediately to the AIJB's Data Protection Officer following the procedures set out in the AIJB's Data Breach Response Plan.

5.6 Information Security

The AIJB's approach to Information Security is set out in its Information Security Policy.

6 Roles and Responsibilities

6.1 Senior Information Risk Owner (SIRO)

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

- Acts as advocate for information risk as a member of the AIJB and the Executive Management Team.
- Drives culture change regarding information risks in a realistic and effective manner.
- Oversees the reporting and management of personal data breaches.

6.2 Data Protection Officer (DPO)

The role of the Data Protection Officer (DPO) is to:

- Inform and advise the AIJB and its employees about their obligations to comply with the data protection legislation.
- Monitor compliance with the data protection legislation, including the assignment of responsibilities, awareness raising and training of staff involved in the processing operations and related audits.
- Provide advice about data protection impact assessments and monitor their implementation.
- Co-operate with the supervisory authority (the Information Commissioner's Office).
- Act as the contact point for the Information Commissioner's Office on issues related to the processing of personal data.
- Coordinate the investigation, mitigation, and reporting of personal data breaches.

- Coordinate response to the exercise of any right by a data subject under the data protection legislation (e.g. subject access requests).

6.3 Information Asset Owners (IAO)

Service 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, are responsible and accountable for all information assets created or managed within their service area. This includes responsibility for the management of any processing of personal data by staff or volunteers within their service, including the sharing of information with any third party by their service.

6.4 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 protecting personal data held or processed by them or which comes within their care, and must comply with this policy and any guidance issued under this policy.

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

7 Governance

7.1 Clinical, Care, and Professional Governance Forum (CCPG)

The CCPG 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 data protection.

This includes:

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

7.2 Partnership Information Governance Working Group (PIGWG)

The IGWG is responsible for the day to day implementation and monitoring of information governance policies and procedures and for promoting information governance best practice across the organisation.

The agreed terms of reference are:

- To communicate/cascade best practice, guidance and information at a service level;

- To regularly review, update, approve (minor changes) and implement the AIJB's information governance policies;
- To implement relevant actions identified in the Information Governance Strategy or any other associated improvement plans;
- To assist with annual Progress Update Reviews for approval by the National Records of Scotland in connection with the AIJB's Records Management Plan; and
- To provide a focal point for the resolution and/or discussion of all information governance issues.

8 Training

All NHS Staff and Angus Council staff carrying out functions on behalf of the AIJB under the direction of the AIJB must, on an annual basis, complete the online e-learning modules on data protection provided by their organisations. All members of the AIJB must also complete basic training in data protection.

9 Monitoring and Reporting

Compliance with this policy shall be monitored by the PIGWG and reported annually to the CCPG.

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

10 Related Policies and Procedures

- AIJB Records Management Policy
- AIJB Information Security Policy
- AIJB Access to Information Policy
- AIJB Data Protection Guidance
- AIJB Data Breach Response Plan
- Tripartite Information Governance Protocol

11 Further Information and Guidance

Data Protection Officer
Angus Health and Social Care Partnership
Angus House
Orchardbank Business Park
Forfar
DD8 1AN

E-mail: AHSCPDataProtection@angus.gov.uk

Appendix 1: The Data Protection Principles

The GDPR sets out six principles for the processing of personal data. Personal data must be:

1. Processed lawfully, fairly and in a transparent manner in relation to the data subject.
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject.
6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

These principles are legally binding on the AIJB and on any person or persons carrying out functions of the AIJB on its behalf.

Appendix 2: Lawful Bases for Processing Personal Data

The lawful bases for processing are set out in Article 6(1) of the GDPR. At least one of these must apply whenever the AIJB processes personal data:

- **Explicit Consent:** the individual has given clear consent for the AIJB to process his/her personal data for a specific purpose.
- **Contract:** the processing is necessary for a contract that the AIJB has with the individual, or because the individual has asked the AIJB to take specific steps before entering into a contract.
- **Legal obligation**: the processing is necessary for the AIJB to comply with the law (not including contractual obligations).
- **Vital interests:** the processing is necessary to protect someone's life.

- **Public interest:** the processing is necessary for the AIJB to perform a task in the public interest or in the exercise of official authority vested in the AIJB.
- **Legitimate interests:** the processing is necessary for the purposes of legitimate interests pursued by the AIJB or a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. However, this basis is not available to processing carried out by the AIJB in the performance of its official tasks: it can only apply to the AIJB when it is fulfilling a different role.

The additional conditions for the lawful processing of special category data are set out in Article 9(2) of the GDPR. These are:

- **Explicit Consent:** the individual has given clear consent for the AIJB to process his/her personal data for a specific purpose and they are legally permitted to do so.
- **Employment and Social Security Law:** Processing is necessary in relation to the rights and duties of the data controller or data subject under this legislation.
- **Vital interests:** the processing is necessary to protect someone's life and the data subject is physically or legally unable to give consent.
- **Membership Organisation:** processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes.
- **Data Already in the Public Domain:** processing relates to personal data which are manifestly made public by the data subject.
- **Legal Proceedings:** processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
- **Substantial Public Interest:** processing is necessary for reasons of substantial public interest on the basis of law.
- **Health and Social Care:** processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of law or pursuant to contract with a health professional.
- **Public Health:** processing is necessary for reasons of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices.
- **Research, Statistics, and Archiving:** processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Appendix 3: Rights of Data Subjects

The GDPR provides individuals with the following rights regarding their personal data:

- The right to be informed about how their information will be used.
- The right of access to their personal data.
- The right to rectification, which is the right to require the AIJB to correct any inaccuracies.
- The right to request the erasure of any personal data held by the AIJB where the AIJB no longer has a basis to hold the information.
- The right to request that the processing of their information is restricted.
- The right to data portability.
- The right to object to the AIJB processing their personal data.
- Rights in relation to automated decision making and profiling.