1. Policy Statement

Irabina Autism Services (hereafter referred to as Irabina) is required to comply with the Australian Privacy Principles (APP) in the *Privacy Act 1988 (Cth)*, the Health Privacy Principles in the *Health Records Act 2001 (Vic)* and the *NDIS Act 2013* and its associated *Rules*.

Irabina is a Victorian NDIS service provider and is required to comply with the *Information Privacy Act 2000 (Vic).* It is acknowledged that Irabina is operating across Commonwealth and Victorian privacy principles. As such, Irabina is required to adhere to the Australian Privacy Principles and the Health Privacy Principles (Victorian) in relation to health information.

In situations where a participant's health information is protected by both Commonwealth and Victorian privacy principles, then Irabina must adhere to the Commonwealth principle as this takes precedence.

The privacy policy is to be adhered to by all Irabina employees and volunteers and read in conjunction with the Irabina Code of Conduct, the Irabina Duty of Care – Child Safety Policy and the Irabina Incident Management Policy and Procedure, referencing in particular the Notifiable Data Breaches Scheme (as outlined within Section 3.15 of this policy).

2. Purpose

The purpose of this policy is to outline how Irabina manages and protects a participant's personal information to ensure compliance with all Commonwealth and Victorian privacy legislation and the NDIS Act 2013.

3. Policy

3.1 Australian Privacy Principle 1: Open and Transparent Management of Personal Information

3.1.1 Irabina will make this policy publicly available on the Organisation's website www.irabina.com .

3.1.2 All participants entering service at Irabina, who request the privacy brochure, will receive it free and in a form that is appropriate.

3.1.3 Enquiries or complaints about the Irabina Privacy Policy can be directed to the designated privacy officer:

The CEO
Irabina Autism Services
52 Stud Rd
BAYSWATER VIC 3153

Or by sending an email to feedback@irabina.com

Or by telephone on (03) 9720 1118

National Relay Service (NRS) for people who are deaf, hard of hearing or have a speech impairment:

TTY users can phone 133677, then ask for 03 9720 1118.

Speak & Listen (speech-to-speech) users can phone 1300 555 727, then ask for

03 9720 1118

Internet relay users can connect to NRS on www.relayservice.com.au then ask for

03 9720 1118

Telephone Interpreter Service (TIS)
Please call 131 450 if you require a language interpreter to contact us.

3.2 Australian Privacy Principle 2: Anonymity And Pseudonymity

3.2.1 When a participant makes an initial inquiry about using Irabina goods and services, employees will give the participant the opportunity of not identifying themselves, or using a nickname, unless it is unlawful or impracticable to do so, prior to using goods and services.

3.2.2 Once the participant has commenced service, Irabina requires accurate personal information. However, if a participant wishes to be identified by using a nickname whilst receiving goods and services, Irabina will give the participant this opportunity, unless it is unlawful or impractical to do so.

3.3 Australian Privacy Principle 3: Collection Of Solicited Personal And Sensitive Information

3.3.1 Irabina only collects personal and sensitive information that is directly related to the legitimate purposes to enable the participant use the goods or services they choose. This includes, but is not limited to, a participant's contact details, date of birth, next of kin information and medical records, and in some instances, limited financial information.

3.3.2 Sometimes, Irabina employees, particularly clinicians, may form the opinion that more information is required about the participant to ensure service planning and service matching will meet the participant's expectations. In these circumstances, Irabina employees (clinicians) will discuss this with the participant in a respectful manner and will seek written consent from the participant prior to obtaining such information in a lawful and fair way. This will be recorded on the Consent for Disclosure of Use of Information form.

3.3.3 Only in exceptional circumstances can information be collected from a third party, unless the third party has been authorised for disclosure at service commencement such as when a participant is not competent or unable to provide information required for care provision. In these circumstances it must be considered unreasonable or impracticable to obtain the information or consent from the individual concerned. Irabina employees (clinicians) should discuss this with the Clinical Services Manager prior to implementing third party information collection and must provide a written file note attached to the participant's file.

3.3.4 Irabina also collects personal information about employees during their employment. The personal information which may be collected includes: name, date of birth, residency status, gender, tax file number, banking details, superannuation details, qualifications, recruitment documentation e.g. referee reports, training attended, performance management framework, and other information.

3.4 Australian Privacy Principle 4: Dealing with unsolicited personal information

3.4.1 On occasions, Irabina employees may receive information about a participant from an unauthorised third party. When this occurs, Irabina will decide, within 14 calendar days, whether the information could have been obtained under APP 3. If Irabina forms the view that it could not, then the unsolicited personal information will be destroyed or the information de-identified.

3.4.2 Where unsolicited personal information would normally be destroyed under Section 4.4.1, Irabina will not destroy and/or de-identify such information if it is considered there is a serious threat to health and safety of the participant or a member of the public or if the destruction or de-identification would contravene Australian law.

3.5 Australian Privacy Principle 5: Notification of the collection of personal information

3.5.1 Irabina will take reasonable steps to ensure that the participant from whom the information is being obtained is aware of:

- Irabina, its address and other contact details;
- how the participant can gain access to the information being collected;
- the purpose for which the information is collected;
- any third parties that Irabina usually discloses the information to;
- any law that requires the particular information to be collected;
- consequences (if any) for the participant if all or part of the information is not provided; and
- whether any personal information needs to be disclosed to overseas recipients.

3.5.2 Irabina employees will take all reasonable measures to ensure that the information received and held is up to date. Records shown to be inaccurate or require updating will be amended and/or updated immediately the need is recognised.

3.6 Australian Privacy Principle 6: Use Or Disclosure Of Personal Information

3.6.1 Irabina will only use a participant's personal information for the purpose that is collected. The only exceptions where personal information will be disclosed are:

- the participant has provided written consent to a secondary use or disclosure;
- lessening or preventing a serious threat to life, health, or safety;
- taking appropriate action in relation to suspected unlawful activity or serious misconduct;
- locating a person reported as missing;
- reasonably necessary for establishing, exercising or defending a legal or equitable claim;
- reasonably necessary for matters of a Commonwealth nature such as the defence force (refer to the APP for specific information);
- necessary for certain Defence Force activities outside Australia;
- conducting research; compiling or analysing statistics; management, funding or monitoring as part of the service agreement that Irabina has entered into;
- disclosure to a legal representative of the participant; or
- disclosing unique characteristics such as fingerprints information to an enforcement body.

3.6.2 When such personal information is disclosed, a written file note must be attached to the participant's file outlining the information disclosed and the reasons for disclosure.

3.7 Australian Privacy Principle 7: Direct Marketing

3.7.1 Irabina will not use or disclose personal information for the purposes of direct marketing, including providing and/or selling participant information to third parties unless the participant has provided written consent for 'opting in' for this specific purpose or it is an obligation within the terms and conditions of a service contract that Irabina has entered into.

3.7.2 Where a participant has consented to 'opt in', the participant can request to 'opt out' of participating in any direct marketing at any time a participant is using or participating in goods and services provided by Irabina.

3.8 Australian Privacy Principle 8: Cross-border disclosure of personal information

3.8.1 Irabina will not disclose personal information about a participant to an overseas recipient unless:

3.8.1.1 The participant has consented to the disclosure.

3.8.1.2 The recipient has made a written commitment to adhere to the Australian Privacy principles and there is no reason to doubt the commitment.

3.8.1.3 A permitted general situation exists such as:

- lessening or prevention a serious threat to life, health or safety;
- taking appropriate action in relation to suspected unlawful activity or serious misconduct.
- locating a person reported as missing; or
- necessary for matters of a Commonwealth nature such as the defence force. Refer to the APP for specific information.

3.9 Australian Privacy Principle 9: Adoption, Use Or Disclosure Of Government Related Identifiers

3.9.1 Irabina will not adopt a government related identifier of a participant as its own identifier of the participant unless the adoption of the government related identifier is required or authorised by law or a court/tribunal order, or a condition of a government service agreement entered into by Irabina.

3.10 Australian Privacy Principle 10: Quality Of Personal Information

3.10.1 Irabina employees will take all reasonable measures to ensure that the information received about the participant that is held is up to date. Records shown to be inaccurate or require updating will be amended and/or updated immediately the need is recognised. Please refer to Australian Privacy Principle 5.

3.11 Australian Privacy Principle 11: Security Of Personal Information

3.11.1 Irabina will take reasonable steps to protect personal information from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

3.11.2 Participant management records (that may include personal, sensitive and health information) are stored securely and are accessible only to those who require the information.

3.11.3 Hard copy personal information will be stored securely and remain accessible only to Irabina employees.

3.11.4 Where Irabina no longer needs the personal information for any purpose for which the information may be used or disclosed, it will take all reasonable steps to destroy or ensure that it is de-identified unless the personal information is part of a State or Commonwealth record, or Irabina is required by or under State or Commonwealth legislation, or a court/tribunal order, to retain the information.

3.12 Australian Privacy Principle 12: Access To Personal Information

3.12.1 If Irabina holds personal information about a participant, Irabina will, on request (whether that be verbal or written) by the participant, give the participant access to the information within 30 calendar days unless Irabina is authorised to refuse access by Section 4.12.2 as it relates to a specific State or Commonwealth legislation.

3.12.2 Irabina may refuse access to a participant based on any of the following:

- giving access would pose a serious threat to life, health or safety of any individual or to public health or public safety;
- giving access would have an unreasonable impact on the privacy of other individuals;
- the request for access is frivolous or vexatious;

- the information requested relates to an existing or anticipated legal proceeding;
- giving access would prejudice negotiations between the organisation and the individual;
- giving access would be unlawful;
- denying access is required or authorised by law or a court/tribunal order;
- giving access would likely prejudice the taking of appropriate action in relation to suspected unlawful activity or serious misconduct;
- giving access would be likely to prejudice an enforcement related activity conducted by, or on behalf of, an enforcement body; or
- giving access would reveal evaluative information in connection with a commercial sensitive decision-making process.

3.12.3 The participant will provide the request to the senior staff member at the site normally accessed. In the event that, for whatever reason, contact regarding a request for information cannot be made to the senior staff member at the site normally accessed, then the participant should contact the designated Privacy Officer in the Office of the CEO as follows:

Office of the CEO
Irabina Autism Services
52 Stud Rd
BAYSWATER VIC 3153

Or by sending an email to feedback@irabina.com

Or by telephone on (03) 9720 1118

3.13 Australian Privacy Principle 13: Correction Of Personal Information

3.13.1 Irabina will take reasonable steps, or at the request of the participant or employees, to correct personal information to ensure that it is accurate, up to date, complete, relevant and not misleading.

3.13.2 When Irabina corrects personal information, it will:

- respond within 30 calendar days, with the time period commencing on the day after the day Irabina receives the request;
- notify other relevant agencies of the correction/change if the correction/change is required to deliver services;
- advise the participant of its reasons, in writing, and the complaint process of Irabina if correction is refused and the option to make an associate statement;
- take reasonable steps to associate a statement with personal information it refuses to correct; and
- not charge an individual for making a request, correcting personal information or associating a statement.

3.13.3 If there is a concern that Irabina may have handled personal information inappropriately, a complaint may be lodged to the Chief Operating Officer, or by contacting designated Privacy Officer in the Office of the CEO.

3.14 Complaints

3.14.1 If an individual wishes to make a complaint in relation to matters relating to this policy, they can do so by either making their complaint in writing and sending it to:

Jane Hancock: The Chief Governance, Risk and Compliance Officer
Irabina Autism Services
52 Stud Road Bayswater 3153

Or by sending an email to feedback@irabina.com

3.14.2 All complaints will be dealt with under the Irabina Feedback and\ Complaints policy and procedure for participants and all employees the Complaints Policy for all other matters.

3.15 The Notifiable Data Breaches (NBD) Scheme

3.15.1 A data breach occurs when personal information that an entity holds is subject to unauthorised access or disclosure, or is lost. Personal information is information about an identified individual, or an individual who is reasonably identifiable. Irabina management, staff and volunteers are aware that information that is not about an individual on its own can become personal information when it is combined with other information, if this combination results in an individual becoming 'reasonably identifiable' as a result.

A data breach may be caused by malicious action (by an external or insider party), human error, or a failure in information handling or security systems.

Examples of data breaches include:

- loss or theft of physical devices (such as laptops and storage devices) or paper records that contain personal information
- unauthorised access to personal information by an employee
- inadvertent disclosure of personal information due to 'human error', for example an email sent to the wrong person
- disclosure of an individual's personal information to a scammer, as a result of inadequate identity verification procedures

3.15.2 The NDB scheme in Part IIIC of the Privacy Act requires entities to notify affected individuals and the Office of the Australian Information Commissioner of certain data breaches. The NDB scheme requires Irabina to notify individuals and the Commissioner about 'eligible data breaches'. An eligible data breach occurs when the following criteria are met:

- There is unauthorised access to or disclosure of personal information held by an entity (or information is lost in circumstances where unauthorised access or disclosure is likely to occur).
- This is likely to result in serious harm to any of the individuals to whom the information relates.
- The entity has been unable to prevent the likely risk of serious harm with remedial action.

3.15.3 Entities must also conduct an assessment if it is not clear if a suspected data breach meets these criteria. The assessment will determine whether the breach is an 'eligible data breach' that triggers notification obligations.

3.15.4 The primary purpose of the NDB scheme is to ensure individuals are notified if their personal information is involved in a data breach that is likely to result in serious harm. This has a practical function: once notified about a data breach, individuals can take steps to reduce their risk of harm. For example, an individual can change passwords to compromised online accounts, and be alert to identity fraud or scams.

3.15.5 to make a complaint in relation to matters relating to NBD scheme they can do so by either making their complaint in writing and sending it to:

The CEO
Irabina Autism Services
52 Stud Rd
BAYSWATER VIC 3153

3.15.6 Irabina management, staff or volunteers who suspect an eligible data breach may have occurred must quickly assess the incident to determine if it is likely to result in serious harm to any individual and follow the Irabina Incident Management Policy and Procedure.

3.15.7 The notification to individuals must include recommendations about the steps they should take in response to the data breach. Irabina staff should notify the OAIC using the online Notifiable Data Breach form on the OAIC website.

4. Key Responsibilities

Role	Responsibility
Chief Executive Officer (CEO)	Responding to all formal requests for information and managing all complaints submitted in accordance with the Policy.
Executive Management/Managers	Ensure that the record storage systems and the documentation being used within their departments or programs comply with the provisions of the above legislation and this Policy.
Team Leaders/Clinicians/ Employees	Ensure compliance with this policy and that information is only managed in accordance with the Policy.
Participants	Irabina will ensure participants are aware of: • the Privacy Policy and where it can be obtained; • the need to provide accurate information including updating/correcting information; and • the consequences of not providing accurate information.

5. Definitions

Term	Meaning
Participant	All end users (parents/guardian/carers, those with ASD and related conditions, Professionals, Schools, etc) of goods or services provided by Irabina or is directly affected by, the services
Sensitive Information	Any part of personal information and includes information Irabina may collect such as racial or ethnic origin, religious beliefs, membership of a professional or trade association, criminal record, or health information.

Term	Meaning
The Notifiable Data Breaches (NBD) Scheme	The NDB scheme in Part IIIC of the Privacy Act requires entities to notify affected individuals and the Office of the Australian Information Commissioner of certain data breaches. The NDB scheme requires Irabina to notify individuals and the Commissioner about 'eligible data breaches'. An eligible data breach occurs when the following criteria are met: • There is unauthorised access to or disclosure of personal information held by an entity (or information is lost in circumstances where unauthorised access or disclosure is likely to occur). • This is likely to result in serious harm to any of the individuals to whom the information relates. • The entity has been unable to prevent the likely risk of serious harm with remedial action.

6. Related Documents

Enrolment form

Feedback and Complaints Policy and Procedure

Incident Management Policy and Procedure

Media Policy

Public Affairs Policy

7. Related legislation

Health Records Act 2001

United Nations Convention on the Rights of the Child

Children, Youth and Families Act 2005

Disability Act 2006

Privacy Act 1988

The National Disability Insurance Scheme Act 2013

The Victorian Child Safety Standards

The National Principles for Child Safety

The Australian Privacy Principles

NDIS (Incident Management and Reportable Incidents) Rules 2018 (Cth)

NDIS (Complaints Management) Rules 2018 (Cth)

NDIS (Code of Conduct) Rules 2018 (Cth)

The Human Rights Framework

National Framework for Protecting Australia's Children 2009-2020

Information Privacy Act 2000

Freedom of Information Act 1982

Ombudsman Act 1973

Public Records Act 1973

Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)

Privacy Amendment (Private Sector) Act 2000 (Cth)

The Office of the Australian Information Commission, the Notifiable Data Breach Scheme (NBD) scheme