

PRIVACY AND CONFIDENTIALITY POLICY AND PROCEDURE

Purpose and Scope

This policy and procedure sets out staff responsibilities relating to collecting, using, protecting and releasing personal information, in compliance with privacy legislation. It applies to all:

- ISP staff;
- aspects of ISP's operations; and
- staff and participant personal information.

This policy and procedure should be read in conjunction with ISP's *Records and Information Management Policy and Procedure*. It meets relevant legislation, regulations and Standards as set out in Schedule 1, Legislative References.

Applicable NDIS Practice Standards

Information Management

Outcome

Management of each participant's information ensures that it is identifiable, accurately recorded, current and confidential. Each participant's information is easily accessible to the participant and appropriately utilised by relevant workers.

Indicators

- Each participant's consent is obtained to collect, use and retain their information or to disclose their information (including assessments) to other parties, including details of the purpose of collection, use and disclosure. Each participant is informed in what circumstances the information could be disclosed, including that the information could be provided without their consent if required or authorised by law.
- Each participant is informed of how their information is stored and used, and when and how each participant can access or correct their information and withdraw or amend their prior consent.

Privacy and Dignity

Outcome

Each participant accesses supports that respect and protect their dignity and right to privacy.

Indicators

- Consistent processes and practices are in place that respect and protect the personal privacy and dignity of each participant.
- Each participant is advised of confidentiality policies using the language, mode of

communication and terms that the participant is most likely to understand.

- Each participant understands and agrees to what personal information will be collected and why, including recorded material in audio and/or visual format.

Interaction of Applicable Legislation and Associated Definitions

Privacy Act 1988 (Cth) - regulates how personal information about individuals is handled. The Act includes thirteen Australian Privacy Principles (APPs). The APPs set out standards, rights and obligations for the handling, holding, use, accessing and correction of personal information. The Act protects the privacy of an individual's information where it relates to Commonwealth agencies and private businesses (including not-for-profit organisations) with a turnover of more than \$3 million. **All** organisations that provide a health service and hold health information (other than in a staff record) are covered by the Act.

Health Information – personal information or an opinion about:

- the health, including an illness, disability or injury, (at any time) of an individual;
- an individual's expressed wishes about the future provision of health services to the individual; or
- a health service provided, or to be provided, to an individual;

that is also:

- Personal Information;
- Other Personal Information collected to provide, or in providing, a health service to an individual;
- Other Personal Information collected in connection with the donation, or intended donation, by an individual of his or her body parts, organs or body substances; or
- genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.

Personal Information – information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- whether the information or opinion is true or not; and
- whether the information or opinion is recorded in a material form or not.

Sensitive Information – personal information or an opinion about an individual's:

- racial or ethnic origin;
- political opinions;
- membership of a political association;
- religious beliefs or affiliations;
- philosophical beliefs;
- membership of a professional or trade association;
- membership of a trade union;
- sexual orientation or practices;
- criminal record;

that is also:

- Personal Information;
- Health Information about an individual;
- genetic information about an individual that is not otherwise health information;

- biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
- biometric templates.

National Disability Insurance Scheme Act 2013 (Cth) – regulates how personal information about NDIS participants is handled by the National Disability Insurance Agency. This limits how the Agency collects and uses personal information and when and to whom information can be disclosed. The Agency must also comply with the *Privacy Act 1988 (Cth)*.

Protected Information – information:

- about a person that is or was held in the records of the Agency; or
- to the effect that there is no information about a person held in the records of the Agency.

Victoria

Privacy and Data Protection Act 2014 (Vic) – regulates how personal information is handled by Victorian public sector agencies.

Personal Information – information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion, but does not include information of a kind to which the Health Records Act 2001 applies.

Sensitive Information – personal information or an opinion about an individual's:

- racial or ethnic origin;
- political opinions;
- membership of a political association;
- religious beliefs or affiliations;
- philosophical beliefs;
- membership of a professional or trade association;
- membership of a trade union;
- sexual preferences or practices; or
- criminal record

that is also personal information.

Health Records Act 2001 (Vic) – regulates how health information is handled by the Victorian public and private sectors.

Health Information –

- personal information or an opinion about:
- the physical, mental or psychological health (at any time) of an individual;
- a disability (at any time) of an individual;
- an individual's expressed wishes about the future provision of health services to them;
- a health service provided, or to be provided, to an individual;
- that is also personal information; or
 - other personal information collected to provide, or in providing, a health service;
 - other personal information about an individual collected in connection with the donation, or intended donation, by the individual of their body parts, organs or body

- substances; or
- other personal information that is genetic information about an individual in a form which is or could be predictive of the health (at any time) of the individual or of any of his or her descendants.

Health service –

- an activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual or the organisation performing it;
- to assess, maintain or improve the individual's health;
- to diagnose the individual's illness, injury or disability;
- to treat the individual's illness, injury or disability or suspected illness, injury or disability; or
- a disability service, palliative care service or aged care service;
- the dispensing on prescription of a drug or medicinal preparation by a pharmacist registered under the Health Practitioner Regulation National Law; or
- a service, or a class of service, provided in conjunction with an activity or service referred to above that is prescribed as a health service.

Private sector service providers must comply with the **Privacy Act 1988 (Cth)** and **Health Records Act 2001 (Vic)** when handling health information.

The **Office of the Health Services Commissioner** conciliates complaints between consumers and health care providers.

Policy

ISP recognises, respects and protects everyone's right to privacy, including the privacy of its participants and staff. All individuals (or their legal representatives) have the right to decide who has access to their personal information.

ISP's privacy and confidentiality practices support and are supported by its records and information management processes (see the *Records and Information Management Policy and Procedure*). Privacy and Confidentiality processes interact with the information lifecycle in the following ways:



All staff are responsible for maintaining the privacy and confidentiality of participants, other staff and ISP.

Procedures

General

The Managing Director is responsible for ensuring ISP complies with the requirements of the *Privacy Act 1988 (Cth)*. This includes developing, implementing and reviewing processes that address:

- why and how ISP collects, uses and discloses personal information;
- what information ISP collects about individuals and its source;
- who has access to the information;
- information collection, storage, access, use, disclosure and disposal risks;
- how individuals can consent to personal information being collected, withdraw or change their consent and change information about them held by ISP;
- how ISP safeguards and manages personal information, including how it manages privacy queries and complaints; and
- how information that needs to be updated, destroyed or erased is managed.

The Managing Director reviews these processes regularly, through annual Privacy Audits (see ISP's *Privacy Audit Form* and *Schedule 2. External Audit and Internal Review Schedule*).

All staff are responsible for complying with this policy and procedure and their privacy, confidentiality and information management responsibilities. Staff must keep personal information about participants, other staff and other stakeholders confidential, in accordance with the confidentiality provisions in their employment or engagement contract.

As per ISP's *Human Resources Policy and Procedure*, all staff must undergo Induction, which includes training in privacy, confidentiality and information management. Staff knowledge and application of confidentiality, privacy and information management processes is monitored on a day-to-day basis and through annual Performance Reviews. Additional formal and on-the-job training is provided to staff where required.

ISP's *Privacy Statement* must be prominently displayed in ISP's premises and] included in ISP's *Participant Handbook* and website.

A full copy of this policy and procedure must be provided upon request.

Photos and Videos

Photos, videos and other recordings are a form of personal information. Staff must respect people's choices about being photographed or videoed and ensure images of people are used appropriately. This includes being aware of cultural sensitivities and the need for some images to be treated with special care.

Information Collection and Consent

Participant Information Collection and Consent

ISP will only request personal information that is necessary to:

- assess a potential participant's eligibility for a service;
- provide a safe and responsive service;
- monitor the services provided; and
- fulfil government requirements for non-identifying and statistical information.

Personal participant information that ISP collects includes, but is not limited to:

- contact details for participants and their representatives or family members
- details for emergency contacts and people authorised to act on behalf participants
- participants' health status and medical records
- medication records
- service delivery intake, assessment, monitoring and review information
- assessments, reviews and service delivery records
- external agency information
- feedback and complaints
- incident reports
- consent forms

Prior to collecting personal information from participants or their representatives, staff must explain:

- that ISP only collects personal information that is necessary for safe and effective service delivery;
- that personal information is only used for the purpose it is collected and is stored securely;
- what information is required;
- why the information is being collected and how it will be stored and used;
- the occasions when the information may need to be shared and who or where the information may be disclosed to;
- the participant's right to decline providing information;
- the participant's rights in terms of providing, accessing, updating and using personal information, and giving and withdrawing their consent; and
- the consequences (if any) if all or part of the information required is not provided.

Participants and their families must be provided with ISP's *Privacy Statement* and informed that a copy of this policy and procedure is available on request.

Staff must provide privacy information to participants and their families in ways that suit their individual communication needs. Written information can be provided in Easy English or explained verbally by staff. Staff can also help participants access interpreters or advocates where required.

After providing the above information, staff must use a *Consent Form* to:

- confirm the above information has been provided and explained; and
- obtain consent from participants or their legal representatives to collect, store, access, use, disclose and dispose of their personal information.

Participants and their representatives or families are responsible for:

- providing accurate information when requested;
- completing Consent Forms and returning them in a timely manner;
- being sensitive and respectful to other people who do not want to be photographed or videoed; and
- being sensitive and respectful of the privacy of other people in photographs and videos when using and disposing of them.

NDIS Audits

ISP complies with the requirements of the *National Disability Insurance Scheme (Approved Quality Auditors Scheme) Guidelines 2018* whereby participants are automatically included in audits against the NDIS Practice Standards. Participants may be contacted at any time by an NDIS Approved Quality Auditor for an interview, or for their participant file and plans to be reviewed.

Participants who do not wish to participate in these processes can notify any staff member, who must inform the Managing Director in writing. Their decision will be respected by ISP and will be documented in their participant file. Upon commencement of any audit process, ISP notifies its Approved Quality Auditor of participants who have opted-out of the audit process.

Staff Information Collection and Consent

Personal staff information that ISP collects includes, but is not limited to:

- tax declaration forms
- superannuation details
- payroll details
- employment / engagement contracts
- personal details
- emergency contact details
- medical details
- NDIS Worker Screening Checks, Police Checks and Working with Children Checks
- qualifications
- First Aid, CPR, Anaphylaxis and other relevant certificates
- personal resumes

Where relevant, forms used to collect the above information will also obtain the staff member's consent to collect, store, access, use, disclose and dispose of their personal information.

Storage

Refer to the *Records and Information Management Policy and Procedure* for details on how ISP securely stores and protects staff and participant personal information.

Access

Staff personal information must only be accessed the Managing Director, who may only access the information if it is required in order to perform their duties.

Staff must only access participants' personal information if it is required in order to perform their duties.

Staff and participants have the right to:

- request access to personal information ISP holds about them, without providing a reason for requesting access;
- access this information; and
- make corrections if they believe the information is not accurate, complete or up to date.

All participant access or correction requests must be directed to a relevant staff member responsible for the maintenance of the participant's personal information. All staff access or correction requests must be directed to the Managing Director. Within 2 working days of receiving an access or correction request, the responding staff member will:

- provide access, or explain the reasons for access being denied;
- correct the personal information, or provide reasons for not correcting it; or
- provide reasons for any anticipated delay in responding to the request.

An access or correction request may be denied in part or in whole where:

- the request is frivolous or vexatious;
- it would have an unreasonable impact on the privacy of other individuals;
- it would pose a serious threat to the life or health of any person; or
- it would prejudice any investigations being undertaken by ISP or any investigations it may be the subject of.

Any participant access or correction requests that are denied must be approved by the Managing Director and documented on the participant's file.

Any staff access or correction requests that are denied must be approved by the Management Team and documented on the staff member's file.

Disclosure

Participant or staff personal information may only be disclosed:

- for emergency medical treatment;
- to outside agencies with the person's permission;
- with written consent from someone with lawful authority; or
- when required by law, or to fulfil legislative obligations such as mandatory reporting.

If a staff member is in a situation where they believe that they need to disclose information

about a participant or other staff member that they ordinarily would not disclose, they must consult the Managing Director before making the disclosure.

Reporting

Notifiable Data Breaches Scheme

The Notifiable Data Breaches (NDB) Scheme is a national scheme that operates under the *Privacy Act 1988 (Cth)*. requires organisations to report certain data breaches to people impacted by the breach, as well as the Australian Information Commissioner.

A data breach occurs when personal information about others is lost or subject to unauthorised access. A data breach may be caused by malicious action, human error or a failure in information management or security systems.

Examples of data breaches include:

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

In addition to harm caused to people who are the subject of data breaches, an incident like this may also cause ISP reputational and financial damage.

Further detail about the NDB Scheme is contained in the [*Data Breach Preparation and Response — A Guide to Managing Data Breaches in Accordance with the Privacy Act 1988 \(Cth\)*](#), published by the Office of the Australian Information Commissioner (OAIC).

ISP’s *Data Breach Response Plan* outlines its strategy for containing, assessing and managing data breach incidents.

Identifying a Notifiable Data Breach

A Notifiable Data Breach, also called an ‘eligible data breach’, occurs when:

- there is unauthorised access to or disclosure of personal information, or information is lost in circumstances where unauthorised access or disclosure is likely to occur;
- the disclosure or loss is likely to result in serious harm to any of the people that the information relates to. In the context of a data breach, serious harm may include serious physical, psychological, emotional, financial, or reputational harm; and
- ISP has been unable to prevent the likely risk of serious harm through remedial action.

All potential or actual data breaches must be reported to the Managing Director, who will determine ISP’s response and whether the breach needs to be reported under the NDB Scheme.

If ISP acts quickly to remediate a data breach and as a result it is not likely to result in serious harm, it is not considered a Notifiable Data Breach.

Responding to a Data Breach

If the Managing Director suspects that a data breach is notifiable under the NDB Scheme, they must make an assessment to determine if this is the case.

All data breach incidents (whether notifiable or not) must be responded to in accordance with ISP's *Data Breach Response Plan* and recorded in ISP's *Incident Register*, with relevant actions tracked in its *Continuous Improvement Register* where appropriate.

Where a breach is referred to the Data Breach Response Team, its response will be based on the following steps:

- **Step 1:** Contain the data breach;
- **Step 2:** Assess the data breach and the associated risks;
- **Step 3:** Notify individuals and the Australian Information Commissioner; and
- **Step 4:** Prevent future breaches.

See ISP's *Data Breach Response Plan* for further detail.

Notifiable Data Breaches Involving More Than One Entity

The NDB Scheme recognises that personal information is often held jointly by more than one entity. For example, one entity may have physical possession of the information, while another has legal control or ownership of it. Examples include:

- where information is held by a cloud service provider;
- subcontracting or brokering arrangements; and
- joint ventures.

In these circumstances, an eligible data breach is considered the responsibility of both entities under the NDB Scheme. However, only one entity needs to take the steps required by the NDB Scheme and this should be the entity with the most direct relationship with the people affected by the data breach. Where obligations under the Scheme (such as assessment or notification) are not carried out, both entities will be in breach of the Scheme's requirements.

Other Reporting Requirements

The Managing Director must immediately notify the NDIS Commission if they become aware of a breach or possible breach of privacy legislation.

Data breaches may also trigger reporting obligations outside of the *Privacy Act 1988*, such as to:

- ISP's financial services provider;
- police or other law enforcement bodies;
- the Australian Securities and Investments Commission (ASIC);
- the Australian Prudential Regulation Authority (APRA)
- the Australian Taxation Office (ATO);
- the Australian Transaction Reports and Analysis Centre (AUSTRAC);
- the Australian Cyber Security Centre (ACSC);
- the Australian Digital Health Agency (ADHA);
- Federal, State or Territory Government departments;
- professional associations and regulatory bodies; and
- insurance providers.

Victorian Protective Data Security Standards

The Victorian Protective Data Security Standards (VPDSS) form part of the Victorian Protective Data Security Framework (VPDSF) and establish 18 high level mandatory

requirements to protect data security across the Victorian public sector, including service delivery organisations.

The standards cover information, personnel, ICT and physical security. Each standard is supported by four protocols. The Standards are regulated by the Office of the Victorian Information Commissioner (OVIC).

While ISP is not required to directly report to OVIC or complete the VPDSS compliance documents published on the OVIC website (which public sector agencies are required to do), it is required to comply with the VPDSS.

To ensure ISP's full compliance with the Standards, the Managing Director will:

- work with the Victorian Government with respect to the risk-based reporting arrangements it is developing to ensure ISP is taking suitable steps to protect participant data;
- to establish an initial cybersecurity baseline, consider implementing the Australian Signals Directorate's 'Essential Eight', which are a prioritised list of practical actions organisations can take to make their computers more secure. More detail can be found at: <https://www.asd.gov.au/publications/protect/essential-eight-explained.htm>;
- assess ISP's compliance with the Essential Eight and remediate any identified gaps;
- subscribe to the 'Stay Smart Online' website at: <https://www.staysmartonline.gov.au>. This website provides advice about smart online behaviour and how to respond to online threats; and
- assess ISP against Question 13 of the Department of Health and Human Services' Organisation Compliance Checklist (regarding protective data security). The checklist can be found at <http://fac.dhhs.vic.gov.au/organisation-compliance-checklist>.

Archiving and Disposal

Refer to the *Records and Information Management Policy and Procedure* for details on how ISP archives and disposes of participants' personal information.

Supporting Documents

Documents relevant to this policy and procedure include:

- *Consent Form*
- *Records and Information Management Policy and Procedure*
- *Data Breach Response Plan*
- *Continuous Improvement Register*
- *Participant Handbook*
- *Privacy Statement*
- *Privacy Audit Form*

Monitoring and Review

This policy and procedure will be reviewed at least every two years by the Management Team. Reviews will incorporate staff, participant and other stakeholder feedback.

ISP's feedback collection mechanisms, such as staff and participant satisfaction surveys, will assess:

- satisfaction with ISP's privacy and confidentiality processes;
- whether stakeholders have received adequate information about privacy and confidentiality; and
- the extent to which participants and their supporters feel their privacy and confidentiality has been protected.

ISP's *Continuous Improvement Register* will be used to record improvements identified and monitor the progress of their implementation. Where relevant, this information will be considered as part of ISP's service planning and delivery processes.

DOCUMENT CONTROL

Endorsement Date:

Last Review Date:

Next Review Date:

This policy and procedure will be reviewed at least 2-yearly and changes endorsed by the Management Team.