



INFORMATION MANAGEMENT POLICY & PROCEDURES

AUGUST 2020



Table of Contents

Glossary of terms.....	3
Policy Purpose.....	4
Scope	4
Statement	5
Roles and Responsibilities	5
Procedure Purpose	8
A Person-Centred Approach at ICAS	8
Information Management	9
Information Management System.....	9
Attachment A	13
Declaration to Maintain	13
Confidentiality	13
Related documents/resources.....	14



Glossary of terms

Term	Definition
Australian Privacy Principles (APPs)	These outline how all private sector and not-for-profit organisations with an annual turnover of more than \$3 million, all private health service providers and some small businesses (collectively called 'APP entities') must handle, use and manage personal information. The APPs are included in the <i>Australian Privacy Act</i> (1988) (Cth).
Confidential information	Any information made available to or generated by ICAS which is not already publicly available or about to become publicly available. All <i>personal information</i> is strictly confidential.
Information	Includes information forming part of a database, and information recorded in a material form or not.
Information Management System	The Australian Standard on Records Management (AS 4390) defines recordkeeping systems as 'information systems, which capture, maintain, and provide access to records over time'. This includes managing both hard copy records and electronic and associated documentation.
Participant	A person who meets the NDIS access requirements.
Personal information (includes sensitive information)	Information or an opinion about an identified individual, or an individual who is reasonably identifiable: <ul style="list-style-type: none"> • whether the information or opinion is true or not • whether the information or opinion is recorded in a material form or not.
Personnel	Anyone, paid or unpaid, who works for or with ICAS. It includes members of the governing body or any other similarly-empowered committee constituted by ICAS.
Policy	A statement of intent that sets out how an organisation should fulfil their vision, mission and goals.
Procedure	A statement or instruction that sets out how a policy will be implemented and by whom.



Policy Purpose

This policy is to ensure that information that we may hold for each participant is identifiable, accurately recorded, current, and confidential. Additionally, each participant can easily access their information, and information held about participants is appropriately used by workers in Individualised Community Access Services (ICAS).

Objectives:

The Information Management policy aims to achieve the following:

- The capturing of informed consent to collect, use, retain participants' information, or to share the information with another party(ies)(including assessments).
- Participants accessing supports from us understand why we collect their information, how we use it, and when we disclose it to another party(ies).
- Participants are aware what information may be disclosed about them without their consent if required or authorised by law.
- Participants are told how we store and use their information, when and how they can access their information, and how they can withdraw or change their current consent.
- We maintain an information management system, which records each participant's information in an accurate and timely manner.
- We store documents with appropriate processes in place for their use, access, transfer, storage, security, retrieval, retention, destruction, and disposal processes, relevant and proportionate to the scope and complexity of the supports that are delivered.

Scope

This policy applies to all employees within ICAS.



Statement

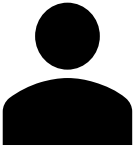
ICAS will ensure that each participant accesses responsive, timely, competent, and appropriate supports to meet their needs, desired outcomes, and goals.

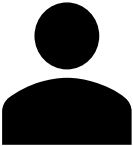
Our **Information Management** policy is based upon:


- Our recognition of the importance of the protecting of information given to us by participants in order to provide appropriate supports to them.
- The need for participants to provide us with consent to collect their information, to use and store it, and to ensure that third parties do not receive information about a participant without that participant's prior consent.
- The acknowledgement that the information we hold belongs to the participant, and that we only collect information to best inform the supports provided.
- The right of the participant to access information we hold about him/her/them.


This policy complies with the requirements under the [National Disability Insurance Scheme \(Quality Indicators\) Guidelines 2018](#) and the [NDIS Code of Conduct](#).

Roles and Responsibilities

Director	Responsibility	Delivery
	Establishing a culture that promotes the recognition of and commitment to a high standard of Information Management practices.	<p>Openly reports on ICAS's commitment to and compliance with our information management policies and procedures.</p> <p>Reviews and identifies issues and encourages staff to make recommendations to implement ongoing continuous improvement.</p> <p>Ensures the Information Management policy is properly administered.</p> <p>Reviews the Information Management policy with management and staff annually.</p> <p>Supports and ensures staff are trained in Information Management processes.</p>

Quality Assurance Officer	Responsibility	Delivery
	<p>Manages and maintains the application of the Information Management processes in day to day operations.</p>	<p>Frequently reports to Director on issues and compliments relating to Information Management policies and procedures for consideration for continuous improvement.</p> <p>Consistently reviews support and staff processes to provide feedback on Information Management opportunities.</p> <p>Ensures there are processes in place for personnel and participants to provide suggestions about the Information Management policies and procedures for continuous improvement.</p> <p>Includes in team and individual staff performance planning processes, indicators that ensure the understanding, and application, Information Management policy and procedures.</p> <p>Analyses compliance with the Information Management policy and procedures across their team and works with the Director to implement quality improvement processes.</p> <p>Supports and encourages staff to deliver record management in accordance with Information Management policies and procedures and delivers mentoring and training where deficits are identified.</p> <p>Provides adequate training to staff to ensure the Information Management policy and procedures are understood and delivered.</p> <p>Acknowledges and rewards staff who demonstrate excellence in demonstrating high levels of compliance with the Information Management policy and procedures.</p>

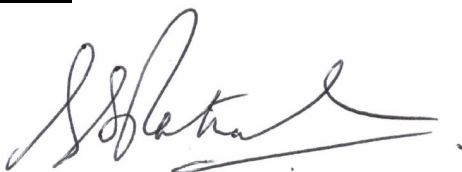
Staff who work with participants	Responsibility	Delivery
	<p>Demonstrates adherence with the Information Management policy and procedures.</p> <p>Attends training on the Information Management policy and procedure.</p>	<p>Comply with the Information Management policy and procedure.</p> <p>Provide feedback to senior management on issues and opportunities relating to the Information Management policies and procedures.</p> <p>Continually seeks to improve the quality of Information Management systems.</p> <p>Actively encourages and supports participants to consider all elements of consent to ensure informed consent.</p> <p>Understand, practice, and deliver the Information Management policy and procedures in working with participants.</p>

All staff	Responsibility	Delivery
	<p>Demonstrates compliance with ICAS's Information Management policy and procedures.</p> <p>Attends training on the Information Management policy.</p>	<p>Comply with the Information Management policy and procedure.</p> <p>Provide feedback to senior management on issues and opportunities to drive continuous improvement in Information Management.</p> <p>Provides suggestions for continuous improvement of the Information Management policies and procedures.</p> <p>Takes active steps to implement changes to the Information Management policy and procedures as required following internal and external audits.</p>

Last Reviewed: 10th August 2020

Last Updated: 10th August 2020

Signed: by Director





Procedure Purpose

These procedures have been developed to provide guidance to all staff in implementing our Information Management policy. ICAS is committed to protecting the rights to independence and informed choice of participants who access our supports.

These procedures provide guidance to staff to ensure that supports accessed by participants through ICAS promotes, upholds, and respects the legal and human rights of participants, including the rights of each participant to receive supports free of violence, abuse, neglect, exploitation and discrimination. In particular, these procedures ensure participants' information is correctly identified, current, and confidential.

This procedure should be read in conjunction with our Information Management Policy and our Privacy and Dignity Policy and Procedures.

A Person-Centred Approach at ICAS

ICAS is committed to a Person-Centred Approach in delivering supports to participants.

Person Centred Supports are central to our philosophy, our mission, and our business model.

Our Person-Centred approach means we will:

- Place participants at the centre of any planning and support process
- Allow participants to choose and direct the support they receive from us in accordance with their aspirations and goals
- Recognise the uniqueness of every participant
- Respect the identity of every participant
- Always focus on the strengths, contributions, and abilities of participants in all our interactions with them and their chosen supporters
- Recognise the participant's chosen supporters as partners
- Work with participants and chosen supporters to maximise personal connection, social participation, personal decision making, and independence.
- Ensure each participant's right to practice their culture, values, and beliefs while accessing supports is facilitated.

We will listen to participants and their chosen supporters in relation to how well we are doing in delivering person centred approaches. This means we will actively respond to their feedback and complaints relating to ensuring person centred approaches are incorporated in everything we do as an ICAS.

We acknowledge the rights to self-determination, dignity, and respect for all people with disability, not only our participants.



Information Management

ICAS is committed to ensuring that information collected from each participant is clearly identified, accurately recorded, current, and confidential. Each participant must have the opportunity to explore context about the use and storage of his/her/their information, and in what situations it may be disclosed. In every case, except those required or authorised by law, we will seek the consent of the participant before disclosing information to any other party. Disclosure will strictly be based on a, 'need to know,' basis. We acknowledge that information we collect about participants is ultimately theirs, and participants may request at any time to see information we hold about them. To assist us in doing this, we maintain an information management system that provides guidance to us on the use, access, transfer, storage, security, retrieval, retention, destruction, and disposal processes relevant and proportionate to the scope and complexity of supports delivered.

Information Management System

PLEASE NOTE THESE PROCEDURES SHOULD BE READ IN CONJUNCTION WITH POLICY AND PROCEDURES PRIVACY AND DIGNITY, WHICH INCLUDES PROCESSES FOR SEEKING INFORMED CONSENT.

Identifying records

Every record must contain a brief, descriptive title and a date to allow collation and filing by subject, in primary groups determined by the quality assurance officer. Important primary groups of files include: governing board meetings, participant files, complaints, incidents, management reviews, internal audits, financial, personnel.

Files of collated records may be electronic (maintained on the intranet) or paper-based. File the records in date order within the primary group. File any sub-groups of records in alphabetical order.

Participants' files are maintained by participant name, and contain individual service agreements, support plans and consents, as well as other records as required.

The Quality Assurance Officer maintains a list of primary groups, files and their location on the intranet.

Access to records

As most of the information collected and held by ICAS (other than public documents, such as policies) are confidential. General access is restricted to personnel who have signed a *Declaration to maintain confidentiality* (Attachment A).

We only collect the personal information that we need to provide supports to participants, when participants approach us initially to ask us about providing those supports; or to comply with relevant legislation. Personal information we may collect, depending on the supports sought, include name, contact details, racial or ethnic origin, religious beliefs or affiliations, sexual orientation or practices, criminal record, and health or other information necessary to provide supports requested.



Personnel do not have unrestricted access to records even if they have signed confidentiality declarations. For example, only personnel specifically authorised to handle and maintain the personal information provided by participants to arrange supports may access participants' files. Such personnel arrange the necessary consents to enable ICAS to provide supports to participants as part of the application process. Other personnel need specific consents to access personal information.

Job descriptions include specific authorities, such as the authority to access participants' files as part of the process of providing supports.

Participants may access their own files in accordance with the *Privacy and Dignity Policy and Procedures*. Participants are able to correct their files if they believe some or all information is inaccurate. If we do not agree with their amendments, a copy of their proposed amendments should still be kept on file.

Only the Quality Assurance Officer or Director may access personnel performance and training files.

Personnel may access their own files in the presence of the Quality Assurance Officer or Director.

Only the Director may access financial or commercial-in-confidence records.

Only personnel with specific authority to investigate complaints and incidents (normally the Director or Quality Assurance Officer) can access such files. This is to ensure confidentiality for complainants and any personnel who may be the subject of a complaint.

When necessary, personnel authorised to access personal information may de-identify information to allow others to view it without the need to obtain additional consents.

Authorised personnel use passwords to access electronic records. Paper records are stored in locked cabinets when not in use.

Privacy and Consent

Personal information may be collected from prospective or current participants communicating with us in the following formats: standard forms in writing, or over the Internet; email, during a telephone conversation with us.

If consent is given at the Support Planning meeting (see Privacy and Dignity policy and procedures) we may collect personal information from other service providers, chosen supporters and/or community members, who the participant requests to be involved. Additional consent will need to be sought to share information with other providers or informal community supports if identified at Service Agreement, Assessment, or Support Planning meetings.

Participants are able to change their mind at any time about consenting to a party accessing their personal information. However, consent will be required to access information that is essential for provision of supports to the participant.



We keep private the data and personal information we collect and hold by following secure handling procedures, ensuring documents are stored in locked cabinets when not in use, and having password protection for electronic files.

Confidentiality

Our personnel must not disclose information about a participant that is identifiable directly or indirectly to that person without the written consent of that person, unless required by law. Where written consent is not available or appropriate, you must facilitate the participant to be supported by a carer, family member or advocate empowered to make an informed decision about consent.

Participant consents must be placed on the participant's individual file. Where a written consent could not be obtained this should be documented on the file.

When we agree to provide supports to a participant, personnel managing provision of the requested supports are required to obtain in advance the consents necessary to provide those supports.

From time to time, additional consents may be sought; for example to allow other personnel to investigate complaints or incidents. If consent is denied, investigation can proceed based on de-identified documents, unless the law requires disclosure.

Participants may withdraw consents at any time. Personnel managing their supports will be aware of consents that are essential for us to provide those supports, and must explain the consequences to participants (and/or their chosen supporters) if withdrawal of consents affects provision of supports.

External auditors need consents to access participants' files or other records containing their personal information, or to interview participants. In this case participants are automatically 'opted in' to the audit process, though always have the right to opt out to involvement in external audits. If participants decide to 'Opt out', this will be documented.

Personnel with different roles in have different levels of access to confidential information. Job descriptions detail what records each position is able to access.

All personnel must therefore be familiar with the Privacy and Dignity policy and procedures and the Information Management policy and procedures to help to meet the expectations that it creates.

We may publish information on our business activities. The following information is not considered confidential:

- Our policies
- Our content on the website.

All other information must be treated as confidential. Note: information that a participant has provided to assist in the delivery of supports is always confidential, unless that participant consents to disclosure (in writing).



All personnel must sign a *Declaration to maintain confidentiality* before they can potentially access confidential information held by us. See Attachment A for the declaration. The declaration will be included in letters of offer for appointment to staff, or as a stand-alone declaration for other staff. The Director holds all signed declarations.

Where participants are unable to provide consent, personnel managing supports for that participant a family member, carer, guardian or advocate who is legally allowed to act on a behalf of a participant can provide consent. All consents as far as possible must be collected in writing and place on the participant's file. Should consent not be given, or written consent not possible, a note must be written on the file.

Record and document retention, archiving and disposal

Our current policy is to retain most records indefinitely. The exception is participants' files, and files which contain participants' personal information, such as records of complaints and incidents. These must be deleted or securely disposed of when no longer required. The maximum retention period is 5 years from the date we cease to provide supports to that participant, or as required by law (whichever is greater).

If the Director or Quality Assurance Officer considers some records containing personal information need to be kept for longer periods (e.g. records of some complaints and incidents), they will ensure that the personal information is de-identified.

Paper records or documents containing confidential information must be disposed of securely by shredding when no longer needed.

If paper records or documents are converted to electronic format, the paper copies may be disposed of, with the approval of the Quality Assurance Officer.

Paper records or documents that are not confidential are recycled.

The Quality Assurance Officer will develop archiving procedures for paper records if required.

Backup and security of electronic data

The Quality Assurance Officer is responsible for backing up the data. Backups comprise of uploading to the cloud immediately, as well as a weekly after hours automatic backup of the entire system to an external hard drive.

An electronic backup log on the computer indicates whether or not the backup process was successful.

The Quality Assurance Officer is responsible for ensuring that appropriate firewalls and other security measures are in place, regularly updated and effective.



Attachment A



Declaration to Maintain Confidentiality

I, _____ (name) hereby acknowledge that:

1. I have read and I understand ICAS's Information Management Policy and Procedure, and Privacy and Dignity Policy and Procedure. I agree to comply with requirements in these documents as they apply to my association with ICAS.
2. I agree to maintain the confidentiality of any information which is not available to the public and which may become known to me by reason of my association with ICAS.
3. I shall not directly or indirectly disclose such confidential information to any third party without the prior written consent of the Director/Senior Manager (or delegate) of ICAS.
4. I shall take reasonable precautions to maintain confidentiality and prevent disclosure of such confidential information.
5. I shall not use, exploit for my own benefit, or improperly use or permit to be used for the benefit of others, any confidential information gained by reason of my association with ICAS.
6. At the termination of my association with ICAS, or before then if requested by ICAS, I agree to return to ICAS any confidential information recorded in a material form in my possession, and which was obtained by reason of my association with ICAS.
7. I agree that my obligations under this declaration shall survive termination of my association with ICAS indefinitely.

Name _____ ICAS Name _____

Signature _____ Signature _____

Date _____ Date _____



Related documents/resources

Applicable NDIS Practice Standards Policies and Procedures

- **Information Management**
- Privacy and Dignity Policy and Procedures
- Governance and Operational Management

Applicable Forms/Registers

- Declaration to maintain confidentiality form
- Document Control Register
- Job Description
- Client Consent Form
- Feedback & Complaints Register
- Incident Register
- Employee Register
- Conflict of Interest Register
- Internal Audit Register
- Continuous Improvement Register
- Delegations Register
- Probity Checks Register
- Staff Handbook
- Client Handbook

Applicable Legislation and NDIS requirements

- [National Disability Insurance Scheme \(Quality Indicators\) Guidelines 2018](#)
- [The Australian Privacy Act \(1988\) Cth](#)
- [NDIS Code of Conduct](#)