Privacy and Information Sharing Policy

Parent document: **UCWB Rules and Regulations**

Document owner: **Executive Director Corporate Services**

Policy category: **Operational – Organisation-wide**

1. Policy Statement

We will collect, store, use information in accordance with the Privacy Act 1988 (which includes the Australian Privacy Principles), and share personal, health and sensitive information in accordance with the Privacy Act 1988 and the SA Government Information Sharing Guidelines where they apply (see section 9.1.4 for details).

2. Purpose

Our purpose is to:

- collect, store and use personal, health and sensitive information in accordance with *the Privacy Act 1988* and the Australian Privacy Principles.
- Use this information to deliver relevant, individually tailored and effective services whilst preserving the privacy of individuals as per legislative requirements
- where circumstances require it, share personal, health and sensitive information in accordance with the *Privacy Act 1988* and SA Government Information Sharing Guidelines to protect the safety and wellbeing of children, young people and vulnerable adults.

3. Scope

This policy applies to all staff (employees, volunteers and contractors) and to information we collect on individuals when we:

- provide services to them
- obtain services from them
- engage them as employees or volunteers.

4. Definitions

Data breach	Unauthorised access to, unauthorised disclosure of, or loss of, personal information held by us. This relates to both physical and electronic records.

Eligible data breach

A data breach where there is unauthorised access to, unauthorised disclosure of, or loss of, personal information held, which is likely to result in serious harm to the person to whom the information relates.

Health information

As defined in the Privacy Act s6FA:

- information or an opinion about:
  - the health, including an illness, disability or injury, (at any time) of an individual; or
  - 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
- 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.

Health service

As defined in the Privacy Act s6FB

An activity performed in relation to an individual is **a *health service*** if the activity is intended or claimed (expressly or otherwise) by the individual or the person performing it:

- to assess, maintain or improve the individual's health; or
- where the individual's health cannot be maintained or improved—to manage the individual's health; or
- to diagnose the individual's illness, disability or injury; or
- to treat the individual's illness, disability or injury or suspected illness, disability or injury; or
- to record the individual's health for the purposes of assessing, maintaining, improving or managing the individual's health.

Permitted health situation

As defined in the Privacy Act 1988, s16B:

A ***permitted health situation*** exists in relation to the collection, use of disclosure of health information about an individual if

- The information is necessary to provide a health service to an individual; and
- Either the collection is required or authorised by or under an Australian Law (other than the Privacy Act 1998) or the information is collected in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation.

Personal information

As defined in the Privacy Act 1988:

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.

Responsible Person

As defined by the *Privacy Act 1988*, s 6AA:

A ***responsible person*** for an individual is:

a parent of the individual; or

- a child or sibling of the individual if the child or sibling is at least 18 years old; or
- a spouse or de facto partner of the individual; or
- a relative of the individual if the relative is:
    I. at least 18 years old; and
    II. a member of the individual's household; or
- a guardian of the individual; or
- a person exercising an enduring power of attorney granted by the individual that is exercisable in relation to decisions about the individual's health; or
- a person who has an intimate personal relationship with the individual; or
- a person nominated by the individual to be contacted in case of emergency.

Sensitive information

As defined in the Privacy Act 1988:

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 of practices
- criminal record

that is also personal information or:

- 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
- biometric templates.

5. Privacy Officer

The Executive Director Corporate Services is the Privacy Officer.

6. Collecting and Storing Information

6.1 Purpose of Collecting Information

6.1.1 Personal information

We collect personal information about a person when we need it to:

- provide services
- comply with legislation
- meet the requirements of government service and funding agreements
- respond to questions or requests for information.

6.1.2 Health Information

We collect health information about a person when we need it to:

- Provide health services
- comply with legislation
- meet the requirements of government service and funding agreements
- undertake research to manage, fund, monitor our health services.

We will only collect health information where a *permitted health situation* exists.

6.1.3 Sensitive information

We may collect sensitive information about a person where the information:

- is necessary to provide the person with a particular service; and
- solely relates to the person who has regular contact with us in connection with a service provided.

6.2 Collecting Information

6.2.1 Personal information other than sensitive information

We will let the person know when we are collecting personal information and the reasons we are collecting it when:

- they contact us to ask for information and / or a response
- we need it to provide a service or information to them
- they provide us with goods or services
- they subscribe to our social media platforms
- they donate to us
- we engage them as employees or volunteers
- they attend events hosted or facilitated by us.

If we receive unsolicited personal information that we could not have reasonably collected ourselves then we will ensure that is it de-identified and destroyed. We may use or disclose the information in order to make this decision.

6.2.2 Sensitive information

We only collect sensitive information about an individual if they consent and it is necessary to provide the person with a particular service, unless an exception exists.

6.2.3 Health information

We only collect health information about an individual if they consent and where a *permitted health situation* exists, unless an exception exists.

6.3 Collecting Without Consent

The *Privacy Act 1988* allows us to collect personal information without obtaining consent where a *permitted general situation* exists, and we reasonably believe we are:

- lessening or preventing a serious threat to life, health or safety
- Taking appropriate action in relation to suspect unlawful activity or serious misconduct
- Locating a person reported as missing
- Specific legal and dispute resolution purposes

Where a *permitted health situation* exists and the person is physically or legally incapable of giving information, the information can be collected from a responsible person acting on their behalf. (See *Definitions* for who is a responsible person).

6.4 Storing Information

We hold personal, health and sensitive information as either a physical or electronic record and have processes in place to ensure it is secure. All electronic records are managed securely with all data stored within Australia's Sovereign borders.

We apply security to personal, health and sensitive information to ensure that it is only accessed by staff who need it to carry out the delivery of services and programs.

We destroy personal, health and sensitive information in a secure way in accordance with our General Records Management Procedure.

6.5 Correcting Information

We will correct personal, health and sensitive information if the person it is about, or their legal guardian asks us to and explains why it is incorrect.

If a person asks us to correct their personal, health and sensitive information, we will first verify that they are the person we hold information on, or their legal guardian.

7. Using Information

7.1 We will use personal, health or sensitive information only for:

- the main purpose we collected it for
- a related purpose
- any purpose required or authorised by law

7.2 Using Personal Information for Direct Marketing:

- We can use personal information *other than sensitive information* for direct marketing by us of other services relevant to the person, where the person would reasonably expect us to use it for this purpose; and
- where a person can opt out and request not to receive direct marketing communications.
- We can use sensitive information for direct marketing purposes if the person has consented to us to use it for this purpose.

We will ensure that the personal information that we collect, use and share is accurate and complete.

8. Access to Our Policy and to Information

8.1 Information about our Privacy and Information Sharing Policy

We provide information to the public and our consumers about this policy on our website and in our Privacy Information Sheet.

We will provide a copy of this policy to any person who asks for it and take reasonable steps to provide it in the format they ask for.

8.2 Access by a Person to their Personal Information

A person can ask for access to the information that we hold on them by writing to the Privacy Officer.

8.2.1 Privacy Officer approves access

The Privacy Officer will approve access if the circumstances meet the requirements in the Privacy Act. The Privacy Officer will ensure that we provide access within 10 working days of the date we receive the request and keep a record of the request and her decision.

8.2.2 Privacy Officer refuses access

The Privacy Officer will refuse access to information where the request doesn't meet the requirements of the Privacy Act. We will notify the person who requested it in writing of the:

- reason access was denied
- process to complain about the decision.

9. Sharing Information

Sharing or disclosing information is when we share or disclose a person's information in a situation other than where they ask for it for themselves.

9.1 Legislative and Other Requirements

9.1.1 Privacy Act

We can only use or disclose personal information for a purpose for which it was collected, or for a secondary purpose if an exception applies. Exceptions include where:

- The person has consented
- The person would reasonably expect us to use or disclose their information

- We are required to or authorised under Australian Law or a court order
- A *permitted general situation* exists in the relation to secondary use or disclosure
- A *permitted health situation* exists in the relation to secondary use or disclosure

9.1.2 National Disability Insurance Scheme Act

The National Disability Insurance Scheme Act requires that we report certain incidents to the NDIS Quality and Safeguards Commission. This means we have a legal obligation to disclose information about individuals. Refer to the following policies for details:

- Client Incident Management Policy
- Restrictive Practices Policy
- Child and Vulnerable Adult Safe Environments Policy.

9.1.3 Children and Young People (Safety) Act

The Children and Young People (Safety) Act requires mandated notifiers to report to the Department for Child Protection if they suspect a child or young person may be at risk. This means we have a legal obligation to disclose information about individuals. Refer to the Child and Vulnerable Person Safe Environments Policy for details.

9.1.4 South Australian Government Information Sharing Guidelines

The guidelines apply only to contracts we have from the State Government. The guidelines say that we can disclose information if we believe on reasonable grounds that the disclosure is necessary to:

- divert a person from offending or harming themselves
- protect a person or groups of people from potential harm, abuse or neglect
- protect service providers in situations of danger
- help service providers more effectively to address risks to safety and wellbeing
- alert other service providers to a person's need for help.

9.2 Sharing with Consent

If a person asks us to share, or agrees to us sharing, their information we will get their consent in writing to:

- share specified information
- with a specific person or organisation
- for a specified purpose

and then share the information in line with the consent.

9.3 Sharing without Consent

The *Privacy Act 1988* allows us to share personal information without obtaining consent where a *permitted general situation* exists, and we reasonably believe we are:

- lessening or preventing a serious threat to life, health or safety
- Taking appropriate action in relation to suspect unlawful activity or serious misconduct
- Locating a person reported as missing
- Specific legal and dispute resolution purposes

Where a *permitted health situation* exists and the person is physically or legally incapable of giving consent, the information can be shared with a responsible person acting on their behalf. (See *Privacy Act 1988*, s 6AA for the definition of a responsible person).

10. Data Breaches

The Privacy Act defines data breaches and eligible data breaches and sets out what we must do in response to them.

The Privacy Officer manages data breaches.

10.1 Identification and Assessment

If any staff member has reasonable grounds to suspect that a data breach has occurred, they must notify the Privacy Officer.

The Privacy Officer will take immediate action to contain the breach and within 30 days of the notification undertake an assessment of whether an eligible data breach has occurred.

10.2 Notification to the Office of the Australian Information Commissioner

If after assessment the Privacy Officer believes that an eligible data breach has occurred, they will immediately notify the Chief Executive

The Chief Executive will:

- confirm whether an eligible data breach has occurred
- assess whether serious harm **is still likely**
- if serious harm is still likely, authorise the lodging of the online data breach statement with the Office of Australian Information Commissioner

notify the contents of the data breach statement to all individuals affected or only those individuals at risk of serious harm.
If neither of these options is practicable, the Chief Executive will ensure that the contents of the data breach statement are published on our website.

10.3 Reporting to the Board

The Chief Executive will report all eligible data breaches to:

- the Board
- UnitingCare SA, in accordance with their Critical Incident Communication Policy .

10.4 Review

The Privacy Officer will conduct a review of all eligible data breaches to identify and implement actions to prevent future breaches.

11. Staff Information

Our corporate induction sessions for all staff include a summary of critical policies including this Privacy and Information Sharing Policy. New staff must read and acknowledge that they have read this policy.

All line managers must ensure that all their staff understand and apply this policy and regularly provide them with reminders of their responsibilities under this policy and the Information Sharing Procedure.

12. Complaints

We will manage all complaints about our handling of personal and sensitive information in accordance with our Complaints Management Policy and Complaints Management Procedure.

13. Responsibilities

Board	Receive reports on eligible data breaches from the Chief Executive
Chief Executive	Receive reports of data breaches from the Privacy Officer Confirm assessment of eligible data breaches by the Privacy Officer Authorise lodgement of the online data breach statement with the Office of Australian Information Commissioner Report eligible data breaches to the Board and UnitingCare SA in accordance with their Critical Incident Communication Policy
Privacy officer	Provide advice to managers on sharing information without consent Approve access to information requests Manage notifications of data breaches
Line managers	Ensure staff are aware of and apply this policy Approve sharing of information without consent
All staff	Notify all suspected data breaches to the Privacy Officer

14. Delegations

The delegations established by this policy are:

Delegation	Delegated to (position)	Reference
Authority to approve lodgement of online data breach statement to the Office of the Australian Information Commissioner	Chief Executive	Section 10.2

15. Relevant Legislation, Policies, Procedures and Other Documents

15.1 Legislation

Children and Young People (Safety) Act 2017 (SA)

National Disability Insurance Scheme Act 2013 (Cth)

Privacy Act 1988 (Cth)

Privacy Regulations 2013 (Cth)

Privacy (Persons Reported as Missing) Rule 2014 (Cth)

Privacy (Tax File Number) Rule 2015 (Cth)

15.2 Policies and Procedures

Child and Vulnerable Adult Safe Environments Policy

Client Incident Management Policy

Client Incident Management Procedure

Complaints Management Policy

Complaints Management Procedure

General Records Management Procedure

Information Sharing Procedure

Information Technology Information Security Procedure

Restrictive Practices Policy

15.3 Other Documents (internal and external)

Australian Privacy Principles Guidelines 2019, Office of the Australian Information Commissioner

Information Sharing Guidelines (South Australian State Government Cabinet Direction, Department of Premier and Cabinet) Aged Care Quality Standards

Australian Service Excellence Standards

National Disability Insurance Scheme Practice Standards

National Disability Insurance Scheme Code of Conduct

National Quality Standard (Education and Care Services)

National Standards for Mental Health Services

UnitingCare SA Critical Incident Communication Policy (May 2022)

16. Privacy Document History

Version No.	Version Date	Next Review Date	Approved By	Summary of Changes
10.1	04/7/22	04/07/2025	Executive	Name changed from Privacy and Information Management Policy to Privacy and Information Sharing Policy Content from Information Sharing Policy moved to this policy Document owner changed Additional definitions included Detail about relevant legislation and the Information Sharing Guidelines added Policy detail added for compliance with legislation Responsibilities section and Relevant Legislation, Policies, Procedures and Other Documents section updated Language simplified
10.0	30/5/19	30/5/22	Executive	Policy updated in line with the NDIS Code of Conduct Added access to and availability of UCWB's Privacy Information or Policy Added reference to use of information for direct marketing Added Delegations
9.0	30/4/18	30/4/18	Board	Policy approval changed to Board level Responsibility for EM Corporate Services to provide periodic reports on compliance to Executive removed. Reporting of breaches to Board added
8.0	12/2017	12/2018	Executive	Compliance requirements updated following amendments to the Privacy Act. Reviewed alongside review of information sharing policy and procedures. Minor wording changes. (annual review required)
7.0	2/2017	2/2019	Executive	Reviewed – no changes required.
7.0	1/2016	1/2018	Executive	Reviewed. Restructured to comply with the requirements of the Australian Privacy Principles. Responsibilities included.
6.0	8/2014	8/2016	Executive	Reviewed. Separated into policy and procedure
5.0	1/2014	1/2016	Executive	Reviewed – no detail recorded
4.0	6/2011	6/2013	Executive	Reviewed – no detail recorded
1.0	12/2005	12/2007	Executive	Document created