

Table of Contents

1. PURPOSE2

2. SCOPE2

3. DEFINITIONS3

4. WHAT TYPES OF INFORMATION DO WE COLLECT AND WHY?9

5. HOW DO WE USE YOUR PERSONAL INFORMATION?12

6. HOW DO WE STORE AND SECURE THE INFORMATION COLLECT?15

7. HOW TO ACCESS AND CONTROL YOUR INFORMATION17

8. NOTIFICATION OF UPDATES TO OUR PRIVACY POLICY18

9. NOTIFIABLE DATA BREACHES18

10. COMPLAINTS18

11. LEGISLATIVE REFERENCES / STANDARDS19

12. RELATED DOCUMENTS19

13. DOCUMENT CONTROL20

APPENDIX 1 – CLIENT INFORMATION REQUEST FORM20

APPENDIX 2 - Overview/Summary of the Privacy Act 1988 (Cth) and Australian Privacy Principles (APPs)24

Please note printed copies are not able to be controlled and the Intranet will always be referred to for the current version.

1. PURPOSE

- 1.1 UnitingSA Ltd ABN 29 335 570 988 (**UnitingSA**, **we**, **our**, **us**) requires certain personal information about our clients, their representatives or others who interact with us to provide our aged care services, NDIS services, and broader recipients of UnitingSA's services. We are committed to protecting the privacy of those with which we interact.
- 1.2 We are bound by the *Privacy Act 1988 (Cth)* (**Privacy Act**) and the *Aged Care Act 2024 (Cth)* (**Aged Care Act**) to protect your rights to personal privacy and to have your personal information protected.
- 1.3 This Policy explains:
- what personal information we collect about you and how;
 - how we use or disclose your personal information with others;
 - how we securely store and protect your personal information; and
 - your rights to access our records of your personal information and how to contact us.
- 1.4 By voluntarily supplying us with your personal information you are agreeing to be bound by this Policy. While we may update our Policy from time to time, the most recent version of this Policy will always be available on our website. If we change the Policy in any material way we will post a notice on our website along with the updated Policy.

We may also contact you via your contact information on file, for example by email, notification or some other equivalent measure.

If you have any queries, concerns or complaints about how we handle your personal information, please speak with a member of staff or contact our Privacy Officer:

Privacy Officer

Email: privacy@unitingsa.com.au
Phone: 08 8440 2255

Postal Address

Attn: Privacy Officer
UnitingSA
70 Dale Street, Port Adelaide SA 5015

2. SCOPE

This Privacy Policy (**Policy**) may apply to you if you are:

- an aged care client (or prospective aged care client);
- a NDIS participant (or prospective NDIS participant);
- a client/consumer or prospective client of broader supports and services provided by UnitingSA;

Please note printed copies are not able to be controlled and the Intranet will always be referred to for the current version.

- an authorised representative or supporter of an aged care recipient, Mental Health Services consumer or a NDIS participant (or a prospective aged care recipient or NDIS participant);
- an employee or job applicant with us, including for volunteer and student placement roles;
- a contractor (including an employee thereof) or associated provider who contracts with us for services;
- a financial partner or donor; or
- any other individual who interacts with us.

This Policy will be monitored and updated to reflect best practice, professional practice standards and guidelines, regulatory, and legislative requirements.

This Policy operates alongside the Information Sharing Procedure which governs how UnitingSA shares information more broadly.

3. DEFINITIONS

Term	Definition
Aged Care Act	Means the <i>Aged Care Act 2024</i> (Cth) and associated rules and regulations.
Associated Provider	Under the new Aged Care Act, which started on November 1, 2025, contractors and third-party providers are now called Associated Providers.
Authorised representative	Means a person appointed as your representative who is authorised to act or make decisions on your behalf, including, but not limited to, an enduring power of attorney, guardian or administrator.
Client	Means a recipient of UnitingSA’s services, which includes, but is not limited to: <ul style="list-style-type: none"> • recipients and consumers of aged care services; and • NDIS participants; and • MHS consumer • CYHS participant • Property & Housing consumer.
Contractors	Means individuals engaged to perform work on behalf of UnitingSA through a third party. Under the new Aged Care Act, which started on November 1, 2025, contractors and third-party providers are now called Associated Providers.
Individual Advocates /	The New Aged Care Act 2024 emphasises the importance of independent aged care advocates to support older individuals in exercising their rights and making informed decisions about their care. The Aged Care Act encourages individuals to engage with and be supported by independent aged care advocates if they choose. This support includes receiving information, education, and advocacy related to accessing or seeking to access funded aged care services.

Please note printed copies are not able to be controlled and the Intranet will always be referred to for the current version.

	In addition, the Aged Care Act introduces the role of registered supporters, which is further defined below.
Informed consent	<p>The process of a client/individual (or their legal representative) voluntarily agreeing to receive care, treatment, or share personal information after being fully informed about:</p> <ul style="list-style-type: none"> • What is being proposed (e.g. a treatment, service, or information sharing) • The benefits, risks, and alternatives • Their right to say no or withdraw consent at any time
NDIS Act	Means the <i>National Disability Insurance Scheme Act 2013 (Cth)</i>
Protected Information under the Aged Care Act 2024	<p>Section 168 of the Act imposes a duty on registered providers to ensure the protection of personal information of individuals receiving funded aged care services.</p> <ul style="list-style-type: none"> • That personal information “must not be used other than” for the delivery of care or for other purposes for which it was given. • Disclosure is limited (e.g. to other providers or with consent) or when required by the Act. • The provider must take reasonable security safeguards against loss or misuse. <p>The Act also defines protected information (in the general index) as:</p> <p>“relevant information is protected information if:</p> <ol style="list-style-type: none"> (a) it is personal information; or (b) it is information (including commercially sensitive information) the disclosure of which could reasonably be expected to found an action by an entity (other than the Commonwealth) for breach of a duty of confidence.” <p>Protected information includes personal information, and also commercially sensitive information (i.e. information whose disclosure might give rise to legal action if improperly disclosed).</p>
Registered Supporter	<p>A person chosen by an older individual to help them make decisions and communicate their wishes. This role is formalised through registration with the Australian Government Department of Health, Disability and Ageing. A registered supporter can help the older person understand information, communicate their wishes, and make informed decisions. They can also request, access, or receive information on the older person's behalf. A supporter is not a substitute for the older person's decision-making. They assist the older person in making their own choices, not make decisions for them, unless in exceptional circumstances, where the supporter is formally authorised to make decisions.</p> <p>An individual registered as a supporter of the older person is further defined under section 37 of the Aged Care Act.</p>

Please note printed copies are not able to be controlled and the Intranet will always be referred to for the current version.

<p>Screening Check Procedure</p>	<p>Means UnitingSA is committed to using integral talent and acquisition strategies to ensure that prospective employees and volunteers are selected according to merit, cultural and team fit, fitness to perform duties and suitability for the role.</p> <p>To ensure any risk of appointing a person to a role is assessed and minimised, of prospective and existing employees, volunteers, students Board members, and temporary labour hire, require a satisfactory NDIS Worker Screening Check. A Department of Human Services (DHS) Working with Children Check (WWCC) or a National Police Check may be required based on the role and or funding obligations.</p> <p>This procedure applies to all prospective and existing employees, students, Board members, temporary labour hire, and volunteers.</p>
<p>Sensitive information under the Privacy Act 1988, Aged Care Act 2024, NDIS Practice Standards, CYHS clients under SA’s Health Care Act 2008 and SA Privacy Principles</p>	<p>Under the Privacy Act, “sensitive information” is a subset of “personal information” and includes information or opinions about an individual’s:</p> <ul style="list-style-type: none"> • racial or ethnic origin • political opinions • membership of a political association • religious or philosophical beliefs or affiliations • membership of a professional or trade association • membership of a trade union • sexual preferences or practices • criminal record • health information • genetic information (not otherwise health) <p>“Sensitive information” under privacy law gets stronger protections (for example, it typically requires consent or has stricter rules for use and disclosure).</p> <hr/> <p>Kinds of information in aged care typically considered “private or sensitive” includes</p> <ul style="list-style-type: none"> • Residence details, living arrangements, who shares their home. • Health status, diagnoses, medical history, disabilities, medication, care needs • Financial information, vulnerabilities (eg debts, assets) • Cultural, linguistic, or background information • Any personal opinions, beliefs, or preferences that fall into the “sensitive” categories above • Any commercially sensitive information relating to providers (as noted by protected information definitions) <hr/> <p>Under both the NDIS Practice Standards and Australian Privacy Law (Privacy Act 1988), sensitive information is subject to strict protection.</p> <p>Examples of Sensitive Information for NDIS participants includes</p>

Please note printed copies are not able to be controlled and the Intranet will always be referred to for the current version.

	<p>1. Health Information</p> <ul style="list-style-type: none"> ○ Medical history ○ Disabilities or diagnoses ○ Treatment plans ○ Psychological reports or assessments ○ Medication details <p>2. Personal Information</p> <ul style="list-style-type: none"> ○ Full name, date of birth ○ Address and contact details ○ Medicare number or NDIS number ○ Emergency contacts or family details <p>3. Support-Related Information</p> <ul style="list-style-type: none"> ○ Individual support plans (ISPs) ○ Goals and progress reports ○ Incident reports ○ Behaviour support plans ○ Funding arrangements or budgets <p>4. Cultural or Demographic Information</p> <ul style="list-style-type: none"> ○ Ethnicity ○ Indigenous status ○ Language spoken ○ Religious beliefs <p>5. Financial Information</p> <ul style="list-style-type: none"> ○ Banking details ○ Invoices or payment records ○ Plan management details <p>6. Legal Information</p> <ul style="list-style-type: none"> ○ Guardianship orders ○ Court documents ○ Consent forms or service agreements
	<p>For Child and Youth Health clients' sensitive information is a specific subset of personal information that is protected under the Privacy Act 1988 (Cth) and relevant state/territory health legislation (eg South Australia's <i>Health Care Act 2008</i>, if applicable). Sensitive information in this context is handled with additional care due to the vulnerability of minors and the nature of health services.</p> <p>Sensitive Information – Child and Youth Health clients includes</p> <p>1. Health & Medical Information</p> <ul style="list-style-type: none"> ● Diagnoses and medical conditions ● Immunisation records ● Developmental assessments ● Disability information ● Mental health notes or behavioural assessments ● Treatment or therapy plans ● Medications prescribed ● Clinical notes and referrals <p>2. Identifying Information</p> <ul style="list-style-type: none"> ● Full name, date of birth, gender ● Medicare number

Please note printed copies are not able to be controlled and the Intranet will always be referred to for the current version.

	<ul style="list-style-type: none"> • Client ID or hospital record number • Residential and family contact details • Photographs (particularly in a medical or service context) <p>3. Cultural and Demographic Information</p> <ul style="list-style-type: none"> • Aboriginal or Torres Strait Islander status • Country of birth • Primary language spoken • Religious or cultural beliefs (e.g. affecting care preferences) <p>4. Family and Social Information</p> <ul style="list-style-type: none"> • Names and details of parents/guardians • Custody or guardianship arrangements • Family health history (e.g. inherited conditions) • Reports or concerns about neglect or abuse • Social worker or child protection involvement <p>5. Education-Related Information</p> <ul style="list-style-type: none"> • School attended • Learning difficulties • Special education needs • Behavioural support plans involving schools <p>6. Legal and Protective Information</p> <ul style="list-style-type: none"> • Court orders (e.g. parenting or protection orders) • Child protection status or history • Consent documentation (especially where a minor is assessed as mature enough to consent) • Reports made to child safety or welfare services <hr/> <p>For Property and Housing clients in South Australia, sensitive information typically includes any personal and financial data that, if improperly disclosed, could impact the client’s privacy, security, or housing situation. This kind of information is protected under laws such as the South Australian Privacy Principles (SAPPs), which align with the Australian Privacy Principles (APPs) under the Privacy Act 1988.</p> <p>Sensitive Information for Property and Housing Clients (SA) includes</p> <p>1. Personal Identifying Information</p> <ul style="list-style-type: none"> • Full name, date of birth • Contact details (address, phone, email) • Proof of identity documents (e.g., driver’s license, passport) • Residential history (previous addresses, rental history) • Family and household composition details <p>2. Financial Information</p> <ul style="list-style-type: none"> • Income details (salary, benefits, pensions) • Bank account and transaction details • Centrelink or government benefit information • Employment status and history • Credit history or reports • Rental payment history <p>3. Housing and Tenancy Information</p> <ul style="list-style-type: none"> • Lease agreements and tenancy contracts
--	---

Please note printed copies are not able to be controlled and the Intranet will always be referred to for the current version.

	<ul style="list-style-type: none"> • Bond information and payments • Maintenance and repair records • Complaints or dispute records • Eligibility assessments for housing support or public housing • Housing needs assessments and support plans <p>4. Health and Disability Information</p> <ul style="list-style-type: none"> • Information related to health conditions or disabilities that affect housing needs • Requests for modifications or special accommodations • Support services involved (e.g., community or disability support workers) <p>5. Legal and Protection Information</p> <ul style="list-style-type: none"> • Court orders related to tenancy or property • Eviction notices or legal disputes • Details of police or protective orders, if relevant <p>6. Cultural and Demographic Information</p> <ul style="list-style-type: none"> • Aboriginal or Torres Strait Islander status • Language spoken at home • Other cultural or social identifiers relevant to housing support <hr/> <p>For Mental Health Services consumers in South Australia, sensitive information covers personal data that, due to its nature, requires strict confidentiality and careful handling. This information is protected under the Privacy Act 1988, South Australian Health Care Act 2008, and other relevant mental health and privacy legislation.</p> <p>Sensitive Information for Mental Health Services consumers (SA) includes</p> <p>1. Personal Identifying Information</p> <ul style="list-style-type: none"> • Full name, date of birth, gender • Contact details (address, phone, email) • Medicare or health insurance numbers • Emergency contact details <p>2. Mental Health Information</p> <ul style="list-style-type: none"> • Diagnoses (e.g., depression, schizophrenia, anxiety disorders) • Psychiatric history and clinical notes • Psychological assessments and therapy notes • Medication details and prescriptions • Crisis or incident reports • Risk assessments (e.g., suicide or self-harm risk) • Treatment plans and progress notes • Hospitalisation and discharge information <p>3. Physical Health Information</p> <ul style="list-style-type: none"> • Relevant physical health conditions • Disability status impacting mental health <p>4. Social and Support Information</p> <ul style="list-style-type: none"> • Family and social circumstances impacting mental health • Referrals to support services or community programs • Social worker or case management notes • Employment and housing status, if relevant
--	--

Please note printed copies are not able to be controlled and the Intranet will always be referred to for the current version.

	<p>5. Legal and Protective Information</p> <ul style="list-style-type: none"> • Guardianship or treatment orders under the Mental Health Act • Court orders related to treatment or custody • Consent or advance care directives • Police involvement or legal disputes related to mental health <p>6. Cultural and Demographic Information</p> <ul style="list-style-type: none"> • Aboriginal or Torres Strait Islander status • Language and cultural background • Religious or spiritual beliefs affecting care
Workforce / Worker	The term 'workforce' or 'worker' is used throughout this Policy which encompasses any person who carries out work for UnitingSA in any capacity, including an employee, supported employee, outworker, contractor or sub-contractor, a labour hire company, a trainee, a work experience student, or a volunteer.

4. WHAT TYPES OF INFORMATION DO WE COLLECT AND WHY?

In the course of providing our services, we collect personal and other information about clients accessing our services, how our clients interact with us, and our people, which includes those who perform work (paid and unpaid) for us, or contractors who perform work on our behalf. We collect personal information through a number of mechanisms, including as set out below.

- 4.1 **Collection from you (our clients, prospective clients, our people and contractors / Associated Providers):** where possible, we will collect the information we require directly from you. We collect and store information that you provide directly to us (either in person, by email, by phone, by website enquiry form, or by any other direct means). This includes:
- 4.1.1 Contact information: such as your name, address, email address, telephone number;
 - 4.1.2 Personal information: such as date of birth, gender and other diversity information, and driver's licence details;
 - 4.1.3 Financial and payment information: such as your payment information (credit card, bank account, etc).
 - 4.1.4 Aged care funding information: if you are an aged care client, this includes aged care access approvals, funding classification and approvals, services received, DVA number, ACAT assessment details, and other sensitive information which we are required by law to collect (see below);
 - 4.1.5 NDIS information: if you are a NDIS participant, this includes information such as, but not limited to funding approvals and classifications, services received, and other sensitive information which we are required by law to collect.
 - 4.1.6 Sensitive or Protected Information: in order to deliver our services to our clients, we collect, and in some instances are required under various legislation (i.e.,

Please note printed copies are not able to be controlled and the Intranet will always be referred to for the current version.

the Aged Care Act) to collect, certain information considered “sensitive information” under the Privacy Act. Further information has been included in Section 3, Definitions.

For our clients or prospective clients: We will only collect this information about you if is required by legislation, Standards or assists us in providing you care or services.

For our employees: To ensure any risk of appointing a person to a role is assessed and minimised, prospective and existing employees, volunteers, students, Board Members, and temporary labour hire, require a satisfactory NDIS Worker Screening Check. A Department of Human Services (DHS) Working with Children Check (WWCC) or a National Police Check may be required based on the role and or funding obligations. This process will be undertaken in line with our Worker Screening Check Procedure.

4.1.7 For clients and employees, we will collect the below information (with your consent) directly from you or where we have consent to collect the information from a third party. We only collect and use this information to provide tailored care and meet our legal requirements. We may collect:

- 4.1.7.1 Racial, Cultural and ethnic origin / information: eg whether you are an Aboriginal or Torres Strait Islander; Language and cultural background, Interpreter requirements.
- 4.1.7.2 Health or genetic information: eg your medical care history (including family history), mental health, vaccination status, disability information, care plans, discharge information /summaries conditions, needs and expressed future wishes regarding care. In some circumstances, Medicare details may be collected.
- 4.1.7.3 Religious/philosophical beliefs or affiliations: eg Religious or spiritual beliefs affecting care etc.
- 4.1.7.4 Criminal record: as part of the NDIS worker screening checks, we obtain the criminal records of employees. UnitingSA obtains the criminal records of employees in all roles in accordance with our Screening Check Procedure.
- 4.1.7.5 Sexual orientation or marital status: eg preferred pronouns, marital status, gender, sex, etc.
- 4.1.7.6 Family and Social Information: eg Names and details of parents/guardians, Custody or guardianship arrangements, Registered Supporters, Family health history (e.g. inherited conditions), Reports or concerns about neglect or abuse, Social worker or child protection involvement, Family and household composition details, Family and social circumstances impacting mental health, Referrals to support services or community programs, Education or employment history or needs, Social worker or case management notes, Employment and housing status, if relevant etc.
- 4.1.7.7 Legal and Protective Information: eg Guardianship or treatment orders under the Mental Health Act, Court orders related to

Please note printed copies are not able to be controlled and the Intranet will always be referred to for the current version.

treatment or custody, Consent or advance care directives, Police involvement or legal disputes related to mental health, Court orders related to tenancy or property, Eviction notices or legal disputes, Details of police or protective orders, if relevant etc.

4.1.7.8 Financial Information eg income details (salary, benefits, pensions), Bank account and transaction details, Centrelink or government benefit information, Invoices or payment records Employment status and history, Credit history or reports, Rental payment history, debts, assets etc.

4.1.7.9 Housing & Tenancy Agreements eg Lease agreements and tenancy contracts, Bond information and payments, Maintenance and repair records, Complaints or dispute records, Eligibility assessments for housing support or public housing, Housing needs assessments and support plans, Hoarding and squalor assessments etc.

4.1.8 UnitingSA has a “**Client Information Request Form**” (See **Appendix 1**) which is utilised to seek consent to obtain personal and sensitive information from clients.

4.2 **Personal Devices:** if you use our services or interact with us through a personal mobile device, we may receive technical information about your device, numbers that identify the device and your location information. This information may be associated with you.

4.3 **Communications:** when you communicate with us, we collect information such as your contact details (such as email address or phone number). We also engage third party services that provide us with information about how you interact with some communications we distribute. You can advise us should you no longer wish to receive communication from us.

4.4 **Digital Platforms:** if you access our services by connecting a social media login (such as Facebook or Google) we may collect information derived, associated or connected with that platform where permitted by the platform’s terms of service. Any information we collect from social media, or other online, platforms is collected in accordance with that platform’s terms and conditions.

4.5 **Automatic:** we may use cookies (small text files stored on your device) to collect information such as your internet protocol (IP) address, server details, internet service provider, and how you interact with our website). This information is not used to personally identify you.

We use third party tools such as Google Analytics and Meta Pixel to track and measure website interaction and provide data that helps us improve our products and services. If you opt-out of third-party tracking technologies or elect to prevent the use of cookies, this may result in the loss of website functionality, restrict your use of the website or delay or affect the way in which the website operates.

4.6 **Surveillance systems:** in order for us to provide you with appropriate security at our sites, camera surveillance systems (such as CCTV) may be used in public areas at our sites and their surrounds. These systems may collect and store personal information about you.

Please note printed copies are not able to be controlled and the Intranet will always be referred to for the current version.

- 4.7 **Through other sources:** where necessary, we may also collect your information from publicly available records or other sources permitted under law to share information about you. This can include information from relatives or other authorised representatives, health service providers or information relating to an individual's credit worthiness and other information from credit providers, subject to legal restrictions. We may do this where it is unreasonable or impractical to collect this information from you.
- 4.8 **Providing someone else's information:** If you provide us with personal information about someone else (such as where you are the authorised representative or supporter for someone who either receives or is seeking to receive care from our services) you must ensure that you are authorised to disclose their personal information to us and that we may collect, store, use and disclose such information for the purposes described in this Policy. Where we request you to do so, you must assist us with any requests by the individual to access or update the personal information you have collected from them and provided to us. If you are someone who does not have a relationship with us but believe that someone has provided your personal information to us, you will need to contact that person for any questions you have about your personal information (including where you want to access, correct, amend, or request that we delete, your personal information).
- 4.9 You have the option of not identifying yourself or interacting with us using a pseudonym to maintain privacy and anonymity. However, this may not be practicable when engaging our services.
- 4.10 You can choose not to provide your personal information, but it may mean that we are unable to provide you with services. If you are a client (or a prospective client), we will not be able to provide you with our services if you choose not to provide us with certain personal information.
- 4.11 If we receive unsolicited personal information, we will determine whether we could have lawfully collected that personal information. If we determine that we could not have lawfully collected the information, we will destroy or de-identify the information as soon as possible.

5. HOW DO WE USE YOUR PERSONAL INFORMATION?

We will only use personal information for managing and conducting our business of delivering care services, for purposes connected with providing those services (this is our **primary purpose**) or where you make a specific request.

You could reasonably expect the **secondary use** or disclosure, and that is related to the primary purpose of collection or, in the case of sensitive information, directly related to the primary purpose and done in accordance with Australian law.

In addition, we may use your information for related purposes, including marketing and fundraising communications, unless you ask us not to.

How we use the information we collect depends, in part, on which services you receive from us and any preferences you have communicated to us. If you would like to restrict how your personal information is handled beyond what is outlined in this Policy, please speak with a member of staff or contact our Privacy Officer.

Please note printed copies are not able to be controlled and the Intranet will always be referred to for the current version.

5.1 Automated Decision Making

- 5.1.1 We may use secure automated decision-making systems or software to assist us in providing our services to you. Where we do so, we will only input your personal information in a way which complies with this Policy.
- 5.1.2 These decisions may involve the use of your personal information. Please contact our Privacy Officer if you do not wish for your personal information to be used in this way. However, you should be aware that making such a request may affect the services with which we can provide you.

5.2 Images

- 5.2.1 Where UnitingSA seeks to use images, videos, testimonials or case studies of individuals for promotional purposes, UnitingSA will obtain informed consent before collecting the content. At the time of consent, individuals will be informed about the general types of use and the channels in which the content may appear.
- 5.2.2 Individuals may withdraw their consent at any time by contacting us. If consent is withdrawn, we will take reasonable steps to stop using the content and to remove it from our active marketing channels. However, once content is published (for example, in print, broadcast or on third-party websites) it may not always be possible to delete it.
- 5.2.3 UnitingSA may seek to take images of clients in a clinical setting (for example, when documenting and monitoring wounds). UnitingSA will obtain informed consent from these clients. Refer to the Aged Care Clinical Photography Procedure.
- 5.2.4 In circumstances where it is difficult to gain individual informed consent, general notice will be obtained. For example, at a large event, notice will be provided to attendees broadly.
- 5.2.5 Special care is given to images and videos of children under 18 years of age. Consent from the child's parent or legal guardian will be sought in these circumstances.

5.3 Sharing of information via Mobile Devices

- 5.3.1 Use of personally owned devices (BYOD) to access the UnitingSA network, corporate email or any other corporate information resource must comply with the Employee Code of Conduct and relevant procedures.
- 5.3.2 Workers must not share client information with others including family members and friends via a mobile device. This may result in a breach of the UnitingSA Privacy Policy and the Notifiable Data Breach (Customer Information) Procedure. A worker will face disciplinary action if a deliberate client data breach occurs.
- 5.3.3 Workers must not take mobile phone photos of clients or workers within social contexts for use in social media etc. without permission of the individuals involved. No photos are allowed that may compromise the personal privacy and dignity of clients or any other person. A worker will face disciplinary action if a deliberate breach of privacy occurs.

Please note printed copies are not able to be controlled and the Intranet will always be referred to for the current version.

5.4 Research studies

UnitingSA worker roles may undertake client research studies. Each participant in these research studies will be informed about the nature of the research and that their participation is completely voluntary and that they are free to withdraw participation from the study at any time.

5.5 Disclosure of personal information to third parties

We may disclose your information to third parties who assist us in providing, managing and administering our services. We may also disclose your personal information where such disclosure is required by law or where you have provided us with consent to such disclosure.

5.5.1 We may disclose your personal information to third parties that:

- 5.5.1.1 Deliver or assist us in providing certain care services and other direct care services including to community service and health providers who provide necessary follow up and ongoing services;
- 5.5.1.2 To assist workers in providing direct care services to our clients;
- 5.5.1.3 Contracted technology and service providers;
- 5.5.1.4 Process information as necessary for providing aged care services or ensuring we comply with the Aged Care Act and our broader legislative requirements, including Government departments;
- 5.5.1.5 Support us in sending you marketing or fundraising communications, unless you ask us not to; Help us fulfil any requests we make on your behalf which require the disclosure of your personal information; or
- 5.5.1.6 Require your personal information for a purpose connected with the delivery of our services or to which you separately consent.

5.5.2 UnitingSA uses third-party service providers, including marketing and analytics platforms such as Google, Meta (Facebook and Instagram) and LinkedIn. These providers may store or process personal information on servers located outside Australia, including in the United States and other regions.

Where this occurs, UnitingSA takes reasonable steps to ensure that any overseas recipients handle personal information in accordance with the Australian Privacy Principles, including through the use of contractual and technical safeguards. These providers also maintain their own privacy policies, which outline how they manage data.

5.5.3 We do not trade personal information to third parties.

5.5.4 In certain circumstances we may be required to disclose your personal information without your consent in order to fulfil our reporting obligations under the Aged Care Act, NDIS Act (such as reporting incidents to regulators), due to contractual requirements (eg SA Health regarding Mental Health Services),

Please note printed copies are not able to be controlled and the Intranet will always be referred to for the current version.

Child Abuse Mandatory reporting, Safeguarding reporting, or to comply with any court orders, subpoenas or other legal process including investigations, if such disclosure is required by law. Where possible and appropriate, we will notify you if we are required by law to disclose your personal information.

6. HOW DO WE STORE AND SECURE THE INFORMATION COLLECT?

6.1 We may store your personal information as:

- 6.1.1 physical files in a secured area; or
- 6.1.2 electronic information or data.

6.2 Security and management of personal information

- 6.2.1 We will take reasonable steps to protect the personal information we hold from misuse, loss, and unauthorised and accidental access, modification, disclosure, destruction, or other action which prevents or otherwise hinders our access to your personal information on a temporary or permanent basis. We do this by:
 - 6.2.1.1 Putting in place physical, electronic, password protection, multi-factor authentication and procedural safeguards in line with industry standards;
 - 6.2.1.2 Requiring any third-party providers to have acceptable security measures to keep personal information secure;
 - 6.2.1.3 Limiting access to the information we collect about you;
 - 6.2.1.4 Imposing confidentiality requirements on our employees;
 - 6.2.1.5 Only providing access to personal information once proper identification and consent has been given; and
 - 6.2.1.6 Policies and procedures including:
 - (a) Notifiable Data Breach (Customer Information) Procedure
 - (b) Email and Internet Procedure
 - (c) Information Security and Governance Policy
 - (d) Information Management Policy
 - (e) Mobile Device Procedure
 - (f) Network Information Management Procedure
 - (g) Closed Circuit Television (Common Areas) Policy
 - (h) Records Management Procedure
 - (i) Customer Information Management Procedure

Please note printed copies are not able to be controlled and the Intranet will always be referred to for the current version.

- 6.2.1.7 The security of information assets is governed through the Information Security Management System based on ISO27001 security standard, and in accordance with our Information Management Policy.
- 6.2.2 While we take all steps reasonable in the circumstances to protect your information, in the unlikely event of a reportable data breach we will notify you and any relevant authorities in accordance with our obligations under the Privacy Act, other laws as necessary, and our Notifiable data breach procedure.
- 6.2.3 We will only keep your personal information for as long as we require it for the purpose for which it was collected. UnitingSA has the following requirements for retention of personal information (and will refer to the [State Records of South Australia](#) for guidance on retention periods)
- **For Aged Care clients:** We are required by the Aged Care Act to retain certain personal information about aged care clients or others for up to 7 years. Beyond the minimum period, it is advisable to keep records indefinitely if there's a risk of litigation
 - **For NDIS participants:** We are required by the **NDIS Act** to retain certain personal information about NDIS participants for 5 years. Beyond the minimum period, it is advisable to keep records indefinitely if there's a risk of litigation
 - **For CYHS clients:** Records related to incidents, illness, injury, or trauma suffered by a child are to be kept until the child is 25 years old. General child records are kept for three years after their last attendance, with some exceptions like specific attendance records for children with disabilities. Child Death Records are kept for seven years after the child's death. Records related to family assistance law complaints must be kept for seven years. Beyond the minimum period, it is advisable to keep records indefinitely if there's a risk of litigation.
 - **For MHS consumers:** seven years after the last entry for adults, or until the client is 25 years old for minors. Beyond the minimum period, it is advisable to keep records indefinitely if there's a risk of litigation.
 - **Residential tenancy records** must be kept for 2 years after the tenancy ends. Records for tax purposes must be kept for 5 years.
- 6.2.4 We may also be required to retain some or all of your personal information for specified periods of time by other legislation, for example under certain laws relating to companies and financial reporting legislation.
- 6.2.5 If we no longer require your personal information, and are not legally required to retain it, we will take reasonable steps to destroy or de-identify the personal information.
- 6.2.6 We keep records of your marketing consent and any opt-out requests for as long as necessary to ensure we respect your preferences. Opt-out records are stored indefinitely so we can continue to honour your request not to receive marketing.

Please note printed copies are not able to be controlled and the Intranet will always be referred to for the current version.

7. HOW TO ACCESS AND CONTROL YOUR INFORMATION

7.1 Accessing the information we hold about you

- 7.1.1 You have rights to access certain information that we hold about you and request correction if it is inaccurate or incomplete. This includes, in addition to documents containing personal information, a variety of records relating to the provision of aged care services under the Aged Care Act.
- 7.1.2 You have the right to receive information about how your personal information has been used or disclosed.
- 7.1.3 If you are an authorised representative, independent aged care advocate or a supporter of an aged care recipient or NDIS participant, you may also be able to make requests on their behalf to access information with their consent. We will comply with all requests for information in accordance with the Aged Care Act.
- 7.1.4 To make a request to access this information please contact us in writing. UnitingSA has a **Client Information Request Form – Appendix 1** which we require clients, supporters or external agencies to utilise to access this information. We will require you to verify your identity and specify what information you wish to access. If eligible, we will endeavour to grant you access to the information within 30 days. The time it takes us to process your request will ultimately depend on the size and complexity of the request. If we require more time or refuse your request, we will notify you with the reasons why and provide information on how to make a complaint.
- 7.1.5 We may refuse access in certain circumstances, as permitted by law, and will explain the reasons in writing. Access can be refused or limited only in certain circumstances, for example:
- If providing access would pose a serious threat to health or safety.
 - If access would have an unreasonable impact on the privacy of others.
 - If the request relates to legal proceedings and is subject to legal professional privilege.
 - If the information was collected for an investigation of unlawful activity.
- 7.1.6 If we accept your request for access, we may charge a fee to cover our costs of processing the application, including retrieving, reviewing and copying any material requested. We will not charge you for the request itself.

7.2 Updating your personal information

We endeavour to ensure that the personal information we hold about you is accurate, complete and up to date. Please complete **Client Information Request Form - Appendix 1** if you believe that the information we hold about you requires correction or is out of date. We endeavour to process any request within 30 days and will provide written reasons if your request is rejected, as well as providing details for making a complaint about the refusal if necessary.

Please note printed copies are not able to be controlled and the Intranet will always be referred to for the current version.

8. NOTIFICATION OF UPDATES TO OUR PRIVACY POLICY

- 8.1 We will advise clients and their support networks of any substantial or material changes to our Privacy policy via the UnitingSA web page, including a link to the updated policy and a “last updated” date.
- 8.2 All new clients will be provided with a copy of our Privacy brochure at onboarding, which will outline 8.1 within it.
- 8.3 We will implement a process to reobtain client consent when there has been a substantial or material change to our Privacy policy, including discussing those changes in detail with the consumer and their carers. Significant changes may include:
- 8.3.1 Material or significant changes to how we collect, use, store, or disclose personal information.
 - 8.3.2 We change data-sharing practices (eg disclosing to overseas parties).
 - 8.3.3 We introduce new uses of personal data not previously covered.
 - 8.3.4 Our changes might affect client trust or consent.

9. NOTIFIABLE DATA BREACHES

UnitingSA has a **Notifiable Data Breach procedure** which outlines the steps that UnitingSA will take in the event of a notifiable data breach, including steps to prevent future breaches.

10. COMPLAINTS

- 10.1 If you are concerned that we have not complied with your legal rights or the applicable privacy laws, please contact a member of staff or our Privacy Officer at privacy@unitingsa.com.au or via phone (08) 8440 2255. If you are an authorised representative or supporter under the Aged Care Act or NDIS Act, you may complain on behalf of the person who nominated you.
- 10.2 Please provide us with a thorough description of your concerns and a response will be provided within a reasonable period. All complaints to the Privacy Officer must be in writing.
- 10.3 When processing a complaint, we will require you to provide us with information to confirm your identity before processing a request related to information we may hold about you.
- 10.4 We expect our procedures will fairly and promptly facilitate your complaint. However, if you remain dissatisfied, you can also contact the Office of the Australian Information Commissioner as follows:

Director of Compliance Officer of the Australian

Please note printed copies are not able to be controlled and the Intranet will always be referred to for the current version.

Information Commissioner
GPO Box 5218
Sydney NSW 2001

For more information on privacy see the [Australian Information Commissioner's website](#).

11. LEGISLATIVE REFERENCES / STANDARDS

- 11.1 Australian Privacy Principles
- 11.2 Privacy Act 1988 (Cth)
- 11.3 Aged Care Act 2024 (Cth) and associated rules and regulations
- 11.4 National Disability Insurance Scheme Act 2013 (Cth)
- 11.5 NDIS Practice Standards,
- 11.6 SA's Health Care Act 2008

12. RELATED DOCUMENTS

- 12.1 Client Information Request Form (Appendix 1)
- 12.2 Privacy policy – Easy Read
- 12.3 Privacy brochure
- 12.4 Worker Screening Check Procedure
- 12.5 Information Security Governance Policy
- 12.6 Information Management Policy
- 12.7 Information Sharing Procedure
- 12.8 Customer Information Management Procedure
- 12.9 Notifiable Data Breach (Customer Information) Procedure
- 12.10 Email and Internet Procedure
- 12.11 Information and Communication Technology Policy
- 12.12 Information Management Policy
- 12.13 Mobile Device Procedure

Please note printed copies are not able to be controlled and the Intranet will always be referred to for the current version.

- 12.14 Network Information Management Procedure
- 12.15 Closed Circuit Television (Common Areas) Policy
- 12.16 Records Management Procedure
- 12.17 Clinical Photography Procedure Aged Care
- 12.18 Customer feedback and complaints management procedure

13. DOCUMENT CONTROL

All records must be retained in accordance with legislation.

Version	Description of change	Approved by	Date approved	Review Due	Owner position title
10.0	Version adopted in September 2021		September 2021	September 2024	
10.1	Reviewed and updated by Legal Firm Cowell Clark to align with legislation.	Board	February 2025	February 2027	Chief People, Partnerships & Quality Officer
11.0	Updates made include: <ul style="list-style-type: none"> • Transferred into new policy template • Updated to align with new Aged Care Act 2024 (Cth) requirements 	Board	30 October 2025	31 October 2027	Chief People, Partnerships & Quality Officer

APPENDIX 1 – CLIENT INFORMATION REQUEST FORM

For access to personal information under the Privacy Act and Aged Care Act 2024 – please complete this form to access / copy / amend or obtain information about your file.

Requestor Details

Please note printed copies are not able to be controlled and the Intranet will always be referred to for the current version.

If you are a Substitute Decision-Maker or External Provider, please attach:

- Proof of authority (eg Enduring Power of Attorney, Guardianship Order, Legal Guardian)
- Consent from the client (if applicable)
- Evidence of employment with external provider or referral documentation and client consent

Type of Request

- Seeking access to view specific file information** (proceed to next section)
- Seeking access to obtain a copy of specific file information** (proceed to next section)
- Seeking to amend my personal information** (please provide further information)

Type of Information Requested

Please specify the type of information you are requesting (tick all that apply):

- Care Plans
- Health Assessments
- Progress Notes
- Incident Reports
- Medication records
- Financial Statements
- Service Agreements
- Other (please specify):

Time Period Requested

Specify the time period for the information requested:

- All available records
- From: _____ To: _____

Delivery Method

Please note printed copies are not able to be controlled and the Intranet will always be referred to for the current version.

How would you like to receive the information?:

- Email (via Secure PDF)
- Registered Mail
(please note that a printing and delivery cost applies and must be received prior to the release of information)
- In-person collection from:
The Privacy Officer
Level 1, 70 Dale Street,
Port Adelaide
- Other (please specify): _____

Declaration

I declare that the information provided is true and correct, and I understand that access will be provided in accordance with the Privacy Act 1998 and Aged Care Act 2024.

Full Name: _____

Signature: _____

Date: _____

Please submit this request form to the attention of the UnitingSA Privacy Officer via:

Postal Address: Attn: The Privacy Officer
 C/O UnitingSA
 P.O. Box 3032
 Port Adelaide, SA 5015

Email: privacy@unitingsa.com.au

You will receive a response to your request within 14 days.

Additional Information – Right to Access Client File

Documents may not be removed from the file but may be photocopied if the information contained relates solely to the client.

Any information or reference to a third party will not be made available unless the third party consents to release. Personal information will only be disclosed to third parties once it has been de-identified e.g. names have been removed.

File access may be arranged at the service under the supervision of an employee at a time

Please note printed copies are not able to be controlled and the Intranet will always be referred to for the current version.

which mutually suits the client, their support person (if applicable) and the employee.

If a client, or their authorised representative, requests an amendment to the information held in their client file, the information may be amended (by way of corrections, deletions or additions) to ensure:

- the information is accurate;
- the information is relevant, up to date, complete and not misleading, taking into account the purpose for which the information is collected and used.

The service may refuse a request to amend information contained in a client file if it is satisfied that the purpose of the amendment does not meet the criteria specified above. If the service decides to refuse to amend the client file, a written reason for the refusal (with the reason relating to the exemptions above) must be given.

UnitingSA can also refuse a client’s access to their personal information if:

- providing access would pose a serious threat to the life or health of any person;
- providing access to the section requested would have an unreasonable impact on the privacy of other people;
- the information relates to legal proceedings (existing or anticipated) between UnitingSA and the person;

Please discuss with the privacy officer for further information and advice.

Privacy Officer use only

Outcome of Request

<p>I, (Name): _____</p> <p>Approve the release of the requested information:</p> <p>Date Approved: _____</p> <p>Comments (if required): _____</p>	<p>Position: _____</p> <p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p>
<p>Date file requested information was released: _____</p>	

Please note printed copies are not able to be controlled and the Intranet will always be referred to for the current version.

APPENDIX 2 - Overview/Summary of the Privacy Act 1988 (Cth) and Australian Privacy Principles (APPs)

Privacy Act 1988 (Cth) – Overview

The Privacy Act 1988 regulates how personal information is collected, used, disclosed, and managed by:

- Australian Government agencies
- Private sector organisations with an annual turnover of \$3 million or more
- Some small businesses (e.g. those handling health info, credit reporting, etc.)

It provides individuals with rights to access and correct their personal information and lays the foundation for the Australian Privacy Principles (APPs).

For the Act in its entirety – link [here](#)

Australian Privacy Principles (APPs) – Summary

There are 13 APPs, and they apply to all organisations covered by the Privacy Act:

1. Open and Transparent Management

- Maintain a clear and accessible privacy policy and take reasonable steps to ensure compliance with the APPs.

2. Anonymity and Pseudonymity

- Allow individuals to remain anonymous or use a pseudonym where lawful and practical.

3. Collection of Solicited Personal Information

- Only collect personal information that is necessary and by lawful and fair means.

4. Dealing with Unsolicited Personal Information

- If you receive personal info without asking for it, determine if you could have collected it lawfully—if not, destroy it.

5. Notification of Collection

- When collecting personal info, notify the individual (or make them aware) of why it's being collected and how it will be used.

6. Use or Disclosure

- Only use or disclose personal information for the purpose it was collected—unless an exception applies (e.g., consent, legal obligation).

7. Direct Marketing

Please note printed copies are not able to be controlled and the Intranet will always be referred to for the current version.

- Do not use personal info for direct marketing unless specific conditions are met (such as consent or an opt-out mechanism).

8. Cross-border Disclosure

- Take reasonable steps to ensure overseas recipients do not breach the APPs when disclosing personal information internationally.

9. Adoption, Use, or Disclosure of Government Identifiers

- Do not use government-related identifiers (like Medicare numbers) for your own purposes.

10. Quality of Personal Information

- Take reasonable steps to ensure personal information is accurate, up-to-date, and complete.

11. Security of Personal Information

- Protect personal information from misuse, interference, loss, and unauthorised access, modification, or disclosure.

12. Access to Personal Information

- Allow individuals to access their personal information upon request, unless a valid exception applies.

13. Correction of Personal Information

- Correct personal information when it's inaccurate, out-of-date, incomplete, irrelevant, or misleading.

For the Principles in its entirety – link [here](#)

Compliance Tips

- Develop and maintain a Privacy Policy aligned with APP 1.
- Implement staff training on privacy obligations.
- Use privacy impact assessments (PIAs) for new projects.
- Secure personal information with appropriate technical and organisational measures.
- Maintain clear processes for data breaches (including compliance with the Notifiable Data Breaches scheme).
- Allow easy access and correction of personal data by individuals.

Please note printed copies are not able to be controlled and the Intranet will always be referred to for the current version.