

Privacy Policy

Background

Privacy underpins human dignity and other key values such as freedom of association and freedom of speech. It has become one of the most important human rights issues of the modern age.

Privacy is a fundamental human right and in Australia, protecting privacy is a statutory obligation with rights and responsibilities stated within the *Privacy Act 1988*. Privacy is an expectation in many of the contractual arrangements we have with our donors and funders.

Uniting Communities has a responsibility to its customers to protect their privacy by taking great care with their personal and sensitive information. We take this level of care seriously and for some of our most vulnerable customers this is one of the few things over which they have any real control.

Policy

Uniting Communities collects information to provide a holistic approach to customer care which includes personal and sensitive information.

All personal and sensitive information relating to our customers gathered by Uniting Communities, will be collected, maintained, used, stored and disposed of in accordance with the *Privacy Act*, and other relevant legislation.

The *Privacy Act* gives greater control to our customers over the way personal and sensitive information is handled by entitling them to:

- know **why** personal and sensitive information is being collected, **how** it will be used and **who** it will be disclosed to
- have the option of **not identifying them as individuals** in certain circumstances
- ask for **access** to personal and sensitive information (including health information)
- stop receiving unwanted **direct marketing**
- ask for **personal and sensitive information** that is incorrect to be **corrected**
- **being able to make a complaint** if it is considered that their personal and sensitive information has been mishandled.

The Privacy Management Framework of the Office of the Australian Information Commissioner (OAIC) provides principles for organisations to achieve compliance and good privacy governance. The Uniting Communities' Privacy Procedures outlines these principles to implement this Policy.

The personal and sensitive information Uniting Communities collects is one of the most valuable elements to being effective in our business. Consistent with the privacy principles of the OAIC, Uniting Communities' staff will consider the following regarding the collection and retention of personal and sensitive information:

- Only use the information for the purpose for which it was explicitly collected
- Collect the minimum amount (rather than collecting anything useful but unnecessary)

- Information we collect and use is accurate, up-to-date, current, complete, relevant and used for the purposes it was collected for when gaining consent
- Keep it for the shortest possible period.

The *Privacy Act* does not apply to Employee Personnel Records as employment related privacy issues are governed by the *Fair Work Act 2009*. While there may not be a specific Uniting Communities' employee related privacy policy the processes to be followed will mostly align with the principles outlined below during the management of these records.

Principles

Uniting Communities is taking a step towards an approach to ensure privacy protections are built into practices, procedures and systems from the start. These are underpinned by our commitment to the Australian Privacy Principles and are detailed in the Privacy Procedures.

- Uniting Communities will ensure that it manages customers' personal and sensitive information in an open and transparent way.
- Where practicable Uniting Communities will provide customers with the option of dealing anonymously or through use of an alias.
- Personal and sensitive information will be collected only when it is necessary to do so, or it directly relates to the functions or activities of Uniting Communities.
- Uniting Communities will abide by the rules as specified in the relevant procedures about what it must do if it receives personal and sensitive information that we did not take any active steps to collect.
- Where Uniting Communities collects personal and sensitive information we will take reasonable steps to notify affected individuals of the purposes of its use and any consequences if the information is not collected. The information collected will be used towards building strong and supportive communities, and helping people to realise their potential and live the best life they can.
- Personal and sensitive information will not be collected for the purpose of direct marketing without consent. All direct marketing communications will include options to unsubscribe.
- Uniting Communities will only share personal and sensitive information with the individuals' consent, unless in circumstances set out in the *Ombudsman SA Information Sharing Guidelines* such as by law or to prevent or lessen a serious threat to safety and wellbeing.
- Uniting Communities will not identify customers using government related identifiers, instead creating our unique customer codes.
- There is an ongoing commitment to maintaining the integrity of personal and sensitive information collected by Uniting Communities to ensure it is accurate, up-to-date, complete and relevant. Uniting Communities will support the individual accessing their personal and sensitive information to provide corrections.
- Uniting Communities will take reasonable steps to protect personal and sensitive information from misuse, interference and loss; and from unauthorised access, modification or inappropriate disclosure. In the event there is a serious breach of the individuals' privacy, Uniting Communities will inform the individual(s) affected and advise how the customer can complain about a breach of their privacy.
- Uniting Communities will take reasonable steps to review the purpose for which personal and sensitive information is being kept and destroy personal and sensitive information when the information is no longer of use or required by law.

Responsibilities

Uniting Communities will ensure all staff comply with the *Privacy Act* and the Australian Privacy Principles as set out in this policy and associated procedures. If we act outside of this we will take immediate action to resolve the situation and take remedial action to prevent such an issue happening again.

The Executive Manager, People, Culture and Marketing is responsible for the implementation and review of Uniting Communities' Privacy Policy, procedures and practices.

The Executive Manager, Services is also the Privacy Contact Officer who will provide oversight and high-level advice relating to all privacy matters, including seeking legal advice when necessary.

Service and Senior Managers will ensure their staff and volunteers, through induction and regular professional development opportunities, comply with the Privacy Policy and associated procedures.

It is the responsibility of all Uniting Communities' staff to comply with the Privacy Policy and procedures in their daily work roles and to raise any concerns or apparent gaps in these procedures with their line manager or Quality Services.

The Executive Manager, Corporate Services is responsible for the overall data and privacy risk management strategy and ensuring the Data Management Plan is carried out for all Uniting Communities (UC) related business.

Governance and oversight of data collection and use will be monitored by the Privacy Steering Group. This will include the review of Privacy Policy and procedures and receiving feedback on the implementation.

A Data Breach Response Team is drawn from the Privacy Steering Group and will convene to respond to suspected serious data breaches. The Executive Manager Services, who is also the Privacy Contact Officer, will Chair the Data Breach Response Team and advise the Chief Executive appropriately of any serious data breach.

Roles and responsibilities are defined further in the associated procedures.

Definitions

For the purposes of this Policy; **customer** includes:

- clients and consumers of Uniting Communities' services
- donors of money and goods
- funders and agents acting on their behalf
- volunteers and non-employees

Employee record means a record of personal and sensitive information relating to the employment of the employee. Examples of personal and sensitive information relating to the employment of the employee are health information about the employee and personal and sensitive information about all or any of the following:

- (a) the engagement, training, disciplining or resignation of the employee;
- (b) the termination of the employment of the employee;
- (c) the terms and conditions of employment of the employee;
- (d) the employee's personal and emergency contact details;
- (e) the employee's performance or conduct;
- (f) the employee's hours of employment;
- (g) the employee's salary or wages;
- (h) the employee's membership of a professional or trade association or trade union membership;
- (j) the employee's recreation, long service, sick, personal, maternity, paternity or other leave;
- (k) the employee's taxation, banking or superannuation affairs.

As specified in the *Privacy Act 1988*:

Personal information is information from which an individual can be identified or whose identity could reasonably be ascertained whether

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

Sensitive information means information or an opinion about an individual's:

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

that is also personal information; or

- health information about an individual; or
- generic information about an individual; or
- biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
- biometric templates.

Links to Policy

[Access and Equity Policy](#)

[Appointment of Staff Policy](#)

[Approval of Research Policy](#)

[Client Case Notes Procedures](#)

[Complaints and Feedback Policy](#)

[Internal Communications Policy](#)

[External Communications Policy](#)

[Performance Management Policy](#)

[Records Management Policy](#)

[Safe Organisation for Children and Young People Policy](#)

[Safe Organisation for Vulnerable Adults Policy](#)

Links to Legislation

[Aged Care Act 1997](#)(Cwlth)

Aged Care Act 1997 (Cwlth), s 96-1, [User Rights Principles](#) 2014

[Children's Protection Act](#) 1993 (SA)

[Coroners Act](#) 2003 (SA)

[Family Law Act](#) 1975

[Health Care Act](#) 2008 (SA)

[Intervention Orders \(Prevention of Abuse\) Act](#) 2009 (SA)

[Listening and Surveillance Devices Act 1972 \(SA\)](#)

[Mental Health Act 2009 \(SA\)](#)

[National Disability Insurance Scheme Act 2013 \(Cwlth\)](#)

[National Disability Insurance Scheme Rules \(Cwlth\)](#)

[Privacy Act 1988 \(Cwlth\)](#)

[Privacy Amendment \(Enhancing Privacy Protection\) Act 2012 \(Cwlth\)](#)

[Public Sector \(Data Sharing\) Act 2016 \(SA\)](#)

[South Australian Public Health Act 2011 \(SA\)](#)

Version and Document Control

Version History

Date	Version	Changes	Author
06 January 2015	Ver 3.0	Published	Naomi Miranda
18 March 2014	Ver 3.1	Published	Naomi Miranda
17 October 2014	Ver 3.2	Published	Naomi Miranda
20 February 2015	Ver 3.2.1	Link repaired	Naomi Miranda
10 August 2015	Ver 3.2.2	Amended to reflect organisational structure as advised by executive management	Naomi Miranda
22 September 2015	Ver 3.3	Published	Naomi Miranda
30 January 2017	Ver 3.4	Published in format aligned to UC branding and new policy and procedure framework	Kevin Lee
	Ver 3.4.1	Privacy Framework project	Naomi Miranda
December 2017	Ver 3.5.1	Revised Privacy Policy	Robyn Sutherland
7 December 2017	Ver 3.5.3	Approved by Exec	Adrian Nippres
14 December 2017	Ver 4.0	Published	Annette Rohde
28 December 2017	Ver 4.0.1	Amended to reflect consultation feedback of privacy procedures	Naomi Miranda and Adrian Nippres
1 March 2018	V 4.01	Approved by Exec	Robyn Sutherland
1 March 2018	V 5.0	Published	Annette Rohde

Status Active

Document Information: S:\CORPORATE\STRATEGIC MANAGEMENT\POLICY\Vital Records-UC-Privacy Policy V5.0 01Mar2018.docx