

# Privacy Policy

## 1. PURPOSE and SCOPE

- 1.1. This Privacy Policy explains how UnitingSA manages the personal information that we obtain and manage.
- 1.2. This Policy applies to all areas and activities of UnitingSA. All employees, volunteers, students, consultants, contractors and agents of UnitingSA must comply with this Policy.
- 1.3. UnitingSA is required by the Privacy Act 1988 (Commonwealth) to comply with the Australian Privacy Principles (APP's) (subject to the other provisions of the Privacy Act). The APP's regulate the manner in which personal information is handled throughout its life cycle, from collection to use and disclosure, storage, accessibility and disposal.

## 2. BACKGROUND

- 2.1. The APP's aim to ensure that organisations that hold information about people handle that information responsibly as well as give the public greater control over the way information about them is managed.

## 3. POLICY

- 3.1. All UnitingSA services will comply with the APP's which regulate how we collect, use, disclose and store personal information and how individuals may access and correct personal information held about them.
- 3.2. UnitingSA is committed to protecting client, employee and stakeholder privacy. UnitingSA services will only use the information that we collect lawfully.
- 3.3. All employees must complete the 'Employee Privacy and Confidentiality Agreement' Form on commencement of employment with UnitingSA.

## 4. PRIVACY PRINCIPLES

### 4.1. CONSIDERATION OF PERSONAL INFORMATION PRIVACY

#### **Principle 1: Open and transparent management of personal information**

UnitingSA services collect and handle a range of personal information for the purposes of providing services or to carry out legislative functions. We also collect some personal information for planning, funding, monitoring and evaluating our services and functions, but where practicable we remove identifying details from information used for these purposes.

#### **Principle 2: Anonymity and pseudonymity**

In some circumstances, services may be able to offer clients access to services, information or products without the client having to identify themselves.

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

This policy requires updating in New Employee Induction Packs when reviews occur.

## Privacy Policy

### 4.2. COLLECTION OF PERSONAL INFORMATION

#### **Principle 3: Collection of personal information**

UnitingSA services only collect personal and sensitive information where that information is required in order to provide an appropriate service.

We recognise that the nature of these services means that much of the information we handle is very sensitive. Employees will ensure access to sensitive information is restricted to only those parties who have a valid need to access. This applies to electronic and hard copy information.

We use personal information about clients:

- To provide services and care provision;
- To assist employees in providing direct care services;
- For administrative requirements;
- To provide information to community services and health providers who provide necessary follow up and ongoing services, if required;
- For benchmarking reporting in a de-identified form;
- To provide data in both an identified and de-identified form to Government agencies in compliance with numerous legislative requirements.

#### **Principle 4: Dealing with unsolicited (not requested) personal information**

If UnitingSA receives unnecessary personal information the service must, within a reasonable period after receiving the information, determine whether or not the service could have collected the information under Australian Privacy Principle 3. If the service does not require the information, it must, as soon as practicable but only if it is lawful and reasonable to do so, destroy the information or ensure that the information is de-identified.

#### **Principle 5: Notification of the collection of personal information**

UnitingSA services must take reasonable steps to notify clients or ensure that the individual is aware that personal information is being collected about him/her using a Consent to Obtain or Release Sensitive information Form.

### 4.3. DEALING WITH PERSONAL INFORMATION

#### **Principle 6: Use or disclosure of personal information**

UnitingSA will only hold personal information about an individual that was collected for a specific purpose (the primary purpose). UnitingSA services will not use or disclose the information for any other purpose (the secondary purpose) unless:

- Third parties where the client consents to the use or disclosure.
- Where required or authorised by law.
- A UnitingSA service reasonably believes that the use or disclosure is necessary to lessen or prevent: a serious and imminent threat to an

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

This policy requires updating in New Employee Induction Packs when reviews occur.

# Privacy Policy

individual's life, health or safety; or a serious threat to public health or public safety.

## **Principle 7: Direct marketing**

UnitingSA will not use personal information about an individual, or disclose the information for the purpose of direct marketing.

## **Principle 8: Cross-border disclosure of personal information**

All information will be protected if transferred outside of Australia using agreed methods.

## **Principle 9: Adoption, use or disclosure of government related identifiers**

UnitingSA services will not use an Australian Government identifier for any individual (e.g. Medicare numbers) as its own.

### 4.4. INTEGRITY OF PERSONAL INFORMATION

#### **Principle 10: Quality of personal information**

UnitingSA will take reasonable steps to ensure that personal information is accurate, complete and up-to-date.

#### **Principle 11: Security of personal information**

UnitingSA will store and protect information from unauthorised access and use suitable physical, electronic and managerial procedures to safeguard and secure the information we collect.

### 4.5. ACCESS TO AND CORECTION OF PERSONAL INFORMATION

#### **Principle 12: Access to personal information**

Clients are able to access personal information that UnitingSA services collect using the Customer Information Management Procedure (Community Services) and the Aged Care Accessing Written Information Procedure.

#### **Principle 13: Correction of personal information**

Clients are able to request the amendment of personal information that UnitingSA services collect using the Customer Information Management Procedure (Community Services) and the Aged Care Accessing Written Information Procedure.

## 5. PERSONAL INFORMATION OF EMPLOYEES, NEW APPLICANTS, VOLUNTEERS, STUDENTS AND CONTRACTORS

5.1. UnitingSA may use this information in assessing employment applications, administration and management of the employee, contractor, volunteer or student, management of health, safety and wellbeing, fulfilling external reporting requirements, internal planning as well as improvement and organisational development.

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

This policy requires updating in New Employee Induction Packs when reviews occur.

## Privacy Policy

5.2. In the case of employees and applicants who agree to be added to the UnitingSA's recruitment database, the information may be used for follow up contact for future job vacancies.

### 6. NOTIFIABLE DATA BREACH (NDB) SCHEME

6.1. UnitingSA will comply with the Notifiable Data Breaches (NDB) government requirements and ensure that procedures are communicated to employees to minimise the occurrence of a breach and should a NDB occur, the breach is identified and dealt with as required by the Privacy Act's NDB scheme.

6.2. The NDB scheme requires UnitingSA to notify affected individuals and the Australian Information Commissioner (Commissioner) in the event of an 'eligible data breach'.

6.3. A data breach is eligible if it is likely to result in serious harm to any of the individuals to whom the information relates. UnitingSA must conduct a prompt and reasonable assessment if there is a suspected eligible data breach. Refer to the Notifiable Data Breach (Client Information) Procedure for further information.

### 7. CONSENT TO USE IMAGES

7.1. UnitingSA services will obtain informed consent for any images of individuals taken for promotional purposes. Services will use consent forms that contain detail about the purposes for which the photograph or video/DVD footage will be used.

7.2. In some circumstances it can be difficult to gain informed consent. In cases where it is intended to take photographs or video footage at a large event, services may consider giving notice to people attending the function that photographs or video footage will be taken and used for specified purposes. Giving notice demonstrates respect for individual privacy and allows an attendee to make arrangements if they are sensitive to the use of their image.

7.3. Specific care should be taken in the publication of photographs or video/DVD images of children. It is recommended that the consent of the child's parent or legal guardian be sought in relation to photographs or video/DVD footage of persons under the age of eighteen.

### 8. PRIVACY AND RESEARCH

8.1. Any client research studies completed by UnitingSA employees or students on placement must comply with privacy principles and each participant is required to sign a Consent Form prior to participation. Participants in the study should be informed in understandable language about three main points:

8.2. The participant(s) should be informed about the nature of the research.

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

This policy requires updating in New Employee Induction Packs when reviews occur.

## Privacy Policy

- 8.3. The participant(s) should be informed that their participation is completely voluntary and that they are free to withdraw from or not participate in the study at any time. Consent must be made without pressure being put on the participant to engage in the study.
- 8.4. The potential consequences of participating or withdrawing should be presented to the participant(s). This includes risks, and limitations of confidentiality.

### 9. INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) SECURITY

- 9.1. UnitingSA will maintain security processes and controls in place to protect personal information including: software security, encryption, network security, testing, back up servers and email security etc.
- 9.2. Employees are educated on physical security and the handling of personal information when working at sites and when working from home.
- 9.3. Employees are educated on ICT and cyber security practices, such as identifying phishing or spear-phishing emails.

### 10. PRIVACY BY DESIGN

- 10.1. UnitingSA will take reasonable steps to implement practices, procedures and systems that will ensure compliance with the APPs. Privacy will be incorporated into business planning, employee training, service priorities, project objectives and design processes, in line with APP1.
- 10.2. When developing or reviewing a project, UnitingSA will consider the need for a privacy impact assessment (PIA). A PIA identifies how a project can have an impact on individuals' privacy and makes recommendations to manage, minimise or eliminate privacy impacts. The Privacy Commission recommend that organisations conduct PIAs as part of their risk management and planning processes.
- 10.3. Personal information security measures will be maintained with the aim to:
- 10.4. Prevent the misuse, interference, loss or unauthorised accessing, modification or disclosure of personal information;
- 10.5. Detect privacy breaches promptly;
- 10.6. Be ready to respond to potential privacy breaches in a timely and appropriate manner.

### 11. HANDLING COMPLAINTS

- 11.1. If an individual wishes to make a complaint about privacy, that person is to contact the Privacy Officer who will investigate the complaint by using the steps described in the UnitingSA Customer Complaints Handling Procedure.

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

This policy requires updating in New Employee Induction Packs when reviews occur.

## Privacy Policy

- 11.2. You can lodge a complaint with us about any breach of our Privacy Policy and our privacy obligations to you by contacting the Privacy Officer / Manager Quality.

Privacy Officer Enquiries

70 Dale St

Port Adelaide SA 5015

PH: (08) 8440 2255

### 12. RECORDKEEPING

- 12.1. All records relating to corporate information must be retained in accordance with the UnitingSA Records Management Procedure.

### 13. DOCUMENTATION

- 13.1. Employee Privacy and Confidentiality Agreement Form  
13.2. Consent to Obtain and Release Private Information Form  
13.3. Agreement to use of Personal Image, Voice, Historical Material and Other Information  
13.4. Photo / Video Consent Form – Adult  
13.5. Photo / Video t Consent Form – Child

### 14. REFERENCES

- 14.1. Privacy Act 1988 (Commonwealth)  
14.2. Australian Privacy Principles  
14.3. Privacy Amendment (Enhancing Privacy Protection) Act 2012  
14.4. Notifiable Data Breach (Customer Information) Procedure  
14.5. Code of Conduct Policy  
14.6. Records Management Procedure  
14.7. Customer Complaints Handling Procedure  
14.8. Network Information Management Procedure  
14.9. Information Sharing Procedure  
14.10. Aged Care Accessing Written Information Guidelines  
14.11. Customer Information Management Procedure (Community Services)  
14.12. Penelope Case Noting Procedure

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

This policy requires updating in New Employee Induction Packs when reviews occur.