



Policy #10	ORG - POL - Privacy
-------------------	----------------------------

Applies to: Whole of Organisation	Version: 6
Specific responsibility: Chief Executive Officer	Date approved: 30/01/2020
Definitions: Refer to Schedule of Definitions	Next review date: 30/01/2022

Policy Statement

Social Futures is committed to protecting and upholding the right to privacy of service users, staff, volunteers, Board members and other stakeholders. In particular we conform to the *Federal Privacy Act (1988)* and *the Australian Privacy Principles* in protecting the rights of people who use our service to privacy in the way we collect, store and use personal information. This applies to all hard copy and electronic records containing personal information, and to discussions of a personal nature.

Summary

We will:

- meet our legal and ethical obligations as an employer and service provider in relation to protecting the privacy of people who use our service, staff, volunteers and other stakeholders
- ensure the people who use our service, staff and volunteers are provided with privacy when they are being interviewed or discussing matters of a personal or sensitive nature
- provide individuals with information about their rights regarding privacy and we obtain consent when collecting, using and releasing personal information
- ensure all staff, Board members and volunteers understand what is required to meet these obligations
- ensure our privacy policy is accessible and provided in the format requested, where reasonable.

We are committed to transparency in our operations and to ensuring we are open to public scrutiny. We must also balance this with upholding the rights of individuals to privacy, and of the organisation to confidentiality on sensitive organisational matters. We require Board members, staff, volunteers and contractors to respect and maintain the confidentiality of our organisation's business, along with the confidentiality of our stakeholders whether individuals, organisations, businesses or government agencies.



Social Futures

Our Approach to Personal Information

We are committed to collecting, keeping and disposing of all personal information in ways that maintain privacy and confidentiality. We maintain secure systems for storing confidential and personal information, including internal records, service user records and unpublished materials.

We will:

- collect and keep information only when it is relevant and necessary to our work
- provide information to people who use our services about how their personal information is managed
- take account of any relevant cultural or religious sensitivities of people using services in the way information about them is collected, stored and used
- provide options to remain anonymous or use a pseudonym, unless an exemption applies
- securely store the records of people who use our services for the required length of time
- transfer or dispose of the records of people who use our services correctly and securely.

Collection, Storage and Use of Personal Information

Personal information is collected electronically, by telephone or in person, or as a hard copy (faxed, posted or personally provided) and scanned or entered into an electronic database. Where information is provided in paper copy, it is either stored in a locked filing cabinet or scanned into an electronic database and shredded. All electronic data including personal banking information will be safeguarded by firewalls with access to data restricted to relevant positions. Systems administrators will be responsible for ensuring access permissions are appropriate to positions held and reflect current employment status.

Social Futures only uses personal information:

- for purposes consistent with the reason it was provided or a directly related purpose
- where required or permitted by law
- where express or implied consent has been provided by the holder of the information.

Records of People Who Use Our Services

We collect personal information directly from people who use our service, or their referral parties where exemptions apply. We may collect name, date of birth, national or cultural identity, address, phone, email, family information, demographic information, health information, and living arrangements. If the enquiry or referral is by a carer, family member or other member of their support network, information on the nature of their relationship to the individual is collected.

This information or data is collected, stored and used for the purposes of:

- ensuring adequate assessment of the needs of people who use our service, and providing service
- providing appropriate follow-up support for people who use our service and their support networks



Social Futures

- program performance and outcomes monitoring, reporting and evaluation (once de-identified)
- improving service design and delivery, advocacy and capacity building (de-identified)
- as program data (de-identified) for sector, funding agency or peak body purposes
- undertaking our internal administrative functions.

Personnel Records

We will maintain accurate and secure records on our Board members, staff, casual employees and volunteers, for internal administration and human resource management purposes. These records will be made available only to authorised officers, the employee (unless exemptions apply), and as required by law. Personal information collected includes staff and volunteer contact details, job applicant details, induction records, incident reports and staff supervision and support notes. We also collect and securely store copies of referee, police and working with children checks, qualifications and credentials, performance management documents, and training records. This information is collected in hard copy or electronically, and securely stored electronically in our secure data system or in hard copy.

Sector Networking, eNews and Other Newsletters

We collect names and postal or email addresses to inform individuals and organisations of particular services or events which may be of interest. We keep this information until individuals choose to unsubscribe from this service. Every directly addressed contact will include a means by which service users and other stakeholders may opt out of receiving further information. We will remove a previous consent to receive communications from us, upon request. Requests may be directed to Executive Manager, Corporate Support on (02) 6620 1800, or write to PO Box 5419 East Lismore NSW 2480. Distribution lists and contacts will be stored in secure databases and not shared without the consent of the individual.

Social Futures will ensure that all host companies holding organisational data on information security management systems, comply with the ISO/IEC 27001:2013 international standard.

Website Data

We may use internet technologies to log information to manage our website and for statistical or systems administration purposes. This information may include the type of browser and operating systems used, Internet Service Providers, the address of referring web sites, computer IP addresses and search terms when using our search engine. We do not use these technologies to collect or store personal information unless express consent is granted. No attempt will be made to identify users and their browsing activities, except as de-identified data or if required by law.

Unsolicited Information



Social Futures

We will protect personal information that is unsolicited with the same rigour as we protect personal information that we intended to collect, and where appropriate we will destroy or de-identify it as soon as practicable.

Disclosure of Personal Information

We will maintain the privacy of the personal information we hold and take reasonable steps to prevent unauthorised access, modification and disclosure.

We do not share personal information with other organisations or third parties unless:

- express consent is granted
- sharing is otherwise required or permitted by law
- it is required on a temporary basis to enable contractors to perform specific functions.

Accessing and Updating Personal Information

We will provide individuals with access to their own personal information when this is reasonable, appropriate and in accordance with applicable privacy laws. We will take all reasonable steps to ensure that the personal information we hold remains accurate, complete and up to date, and will amend our records when advised of a change of details. Service users may request to have their personal information amended by signing a consent to exchange and release form, or otherwise request in writing (subject to some exceptions allowed by law). Requests to access or amend personal information may be made to Executive Manager, Corporate Support on (02) 6620 1800, or write to PO Box 5419 East Lismore NSW 2480.

Contractors and External Service Providers

We will ensure that our contractual arrangements with these third parties protect the personal information of people who use our service, other stakeholders and other confidential material in compliance with privacy laws. When we temporarily provide personal information to companies who perform services for us, we require those companies to protect personal information as diligently as we do. Contractual and other quality assurance measures are used to ensure personal and confidential information is protected.

Online Security and Privacy

We will ensure our website and online interactions with individuals and organisations are as secure as dealings in person or on the telephone. For site security purposes, and to ensure our online services remain available to all users, we may employ software programs to monitor network traffic in order to identify unauthorised attempts to upload or change information, or otherwise cause us damage.

Overseas Use and Disclosure



Social Futures

We do not transfer or disclose personal information to recipients in countries outside Australia.

Loss of Personal Information

Where a breach of security occurs, or in the event of loss of personal information, we will

- seek to rapidly identify and secure the breach to prevent any further breaches
- engage the appropriate authorities where criminal activity is suspected
- document and assess the nature and severity of the breach including the type of personal information involved and the risk of harm to affected individuals
- notify the affected individuals directly if appropriate and where possible
- notify the Privacy Commissioner (at the OAIC) if the breach is significant.

Notification of 'Eligible Data Breaches'

An eligible data breach is a breach where 'a reasonable person would conclude that there is a likely risk of serious harm to any of the affected individuals as a result of the unauthorised access or unauthorised disclosure' of personal data. Serious harm could include serious physical, psychological, emotional, economic and financial harm, and serious harm to reputation.

We recognise data breaches may fall into two (2) primary categories, serious (eligible) and minor. To ensure that breaches are responded to in an appropriate timely manner a Data Breach Response Plan will be implemented. Minor breaches are those that are rectified quickly and individuals are not at risk of suffering serious harm.

Eligible data breaches will result in immediate notification to individuals affected and to the Officer of the Australian Information Commissioner (OAIC).

Complaints

Any individual may complain about a breach of their privacy or of the Australian Privacy Principles. We will ensure complaints are recorded and promptly and fairly dealt with in accordance with our documented complaints policy and procedures.

E.U. citizens have the right to lodge a complaint with a supervisory authority (Data Protection Authority in your jurisdiction) in case of a breach of any E.U. Data Protection and Privacy Regulations. If the supervisory authority fails to deal with a complaint or inform you within the time frame set under applicable law, you have the right to an effective judicial remedy.



Policy Administration

Policy context: This policy relates to	
Standards or other external requirements	Australian Service Excellence Standards C.2.2 Family Relationships Services Standards 12 National Home Care Standards 3.2
Legislation or other requirements	<i>Refer to Table 1 (Legislation)</i> Privacy Act 1988 (Cth) Children and Young Person Care and Protection Act, 1998 Privacy and Personal Information Protection Act 1998 (NSW) The European Union General Data Protection Regulation (the GDPR)- Regulation (EU) 2016/679

Reviewing and approving this policy		
Frequency	Person responsible	Approval
2 years	Chief Executive Officer	Board

Policy review and version tracking			
Review	Date Approved	Approved by	Next Review Due
1	21/08/2014	Board	28/05/2015
2	28/05/2015	Board	25/08/2016
3	25/08/2016	Board	22/02/2018
4	07/08/2018	Board	25/07/2019
5	18/10/2018	Board	31/10/2019
6	30/01/2020	Board	30/01/2022

Documentation

Documents related to this policy	
Related policies	Legal and Contractual Compliance Information and Knowledge Management Risk Management Employment Conditions Grievance Feedback and Complaints
Related procedures	Risk Management Framework



Social Futures

	Practice Framework Data Breach Response Plan
--	---