SOCIAL FUTURES

Policy #7a	ORG - POL - Privacy, Information and Knowledge Management

Applies to: Whole of Organisation	Version: 2
Specific responsibility: Chief Executive Officer	Last Date approved: 4/10/2022
Definitions: Refer to Schedule of Definitions	Next review date: 4/10/2023

Policy Statement

Social Futures collects and uses information and knowledge, including about our participants, staff, volunteers and stakeholders. This enables us to understand needs, inform our planning and practice, provide services, and monitor/review our performance. It also enables us to produce accurate and timely reports to funding and other bodies, in accordance with our legal and regulatory requirements. We have systems and processes to manage information and knowledge (including personal and confidential information) securely, legally and ethically and to ensure it is accurate, complete and up to date.

Social Futures protects and upholds the right to privacy of participants, staff, volunteers, Board members and other stakeholders. We conform to the *Federal Privacy Act (1988), other relevant legislation listed in this policy* and *the Australian Privacy Principles* in the way we collect, store and use personal and sensitive information. This applies to all hard copy and electronic records containing personal information and to discussions of a personal nature.

Personal information is information or an opinion about an identified individual – for example, name, signature, address, telephone number, date of birth or other identifying information. It may include (but is not limited to) information about participants and their records of service, personnel records* and financial/banking information. It can encompass sensitive information including: health or genetic information; sexual orientation or practices; gender identity; intersex status and or relationship status; racial or ethnic origin; political opinions and membership of a political association; religious beliefs or affiliations; philosophical beliefs; membership of a professional or trade association; membership of a trade union; and criminal record.

Privacy and Confidentiality

We will:

- provide individuals with information about their rights regarding privacy and about how their personal information is managed
- ensure all staff, Board members and volunteers understand our privacy obligations, procedure and processes for the collection, storage, retrieval and transfer of information we hold
- ensure our policy on Privacy, Information and Knowledge Management is accessible and

provided in the format requested, where reasonable.
- ensure participants, staff and volunteers are provided with privacy when they are being interviewed or discussing matters of a personal or sensitive nature

We commit to operate transparently and being open to public scrutiny. We 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.

Personal Information

We collect, retain and dispose of all personal information in ways that maintain privacy and confidentiality and take reasonable steps to prevent loss, unauthorised access, misuse, modification, interference and disclosure. We will:

- collect, hold and use personal information only when it is relevant and necessary to our work and in a way that is lawful and fair
- take reasonable steps, before or at the time of collection (or if not practicable, as soon as possible after collection) to ensure the individual is aware of the fact and circumstances of collection, the purpose of the collection and the consequences if personal information is not collected.
- obtain consent from the holder of the information or their nominated representative when collecting personal sensitive information.
- obtain consent to the use and disclosure of personal information unless an exemption exists in law such as to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety.
- use personal information for the reason it was provided or a directly related purpose
- use / share personal information for purposes where required or permitted by law
- collect personal information only from the person themselves or their nominated representative except where the law exempts this.
- take account of any relevant cultural or religious sensitivities of participants in the way personal information about them is collected, stored and used
- provide options to remain anonymous or use a pseudonym, unless an exemption applies
- retain participant records for the required length of time and store, transfer or dispose of them correctly and securely
- store personal information in an electronic database (including scanned paper records that are subsequently shredded). No paper records of participant information will be retained.
- safeguard electronic data by firewalls with access restricted to relevant positions
- ensure data access permissions are appropriate to positions held / employment status
- protect unsolicited information with the same rigour as other personal information, and where appropriate and lawful, we will destroy or de-identify it as soon as practicable.
- not transfer or disclose personal information to recipients in countries outside Australia

We will provide individuals with access to their own personal information when this is appropriate and consistent with applicable privacy laws. Individuals may request in writing to have personal information amended (subject to some exceptions allowed by law).

Participant Records

We collect personal information directly from participants, 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, sexual orientation, gender identity, intersex status and/or relationship status 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 is used to assess needs and provide appropriate support. Deidentified data is also used to improve programs, report to funders, advocates, to build capacity and for internal administrative functions.

Contractors and External Service Providers

We will ensure that our contractual arrangements with third party contractors and external service providers protect the personal information of participants, 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.

Personnel Records

We will maintain secure records on our Board, staff 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 contact details, job applicant details, induction records, incident reports and staff supervision and support notes. We also collect copies of referee and probity checks, qualifications and credentials, performance management documents, and training records.

Sector Networking, Newsletters and Marketing

We collect names and details of individuals and organisations to inform them of services or events. We keep this information until individuals unsubscribe. Every contact will provide a means for individuals to opt out of receiving further information and will contain our contact details. We will remove a previous consent to receive communications from us, upon request. Distribution contacts will be stored in secure databases and not shared without the consent of the individual. We will ensure that all Social Futures data hosted by external companies complies with international standard ISO/IEC 27001:2013.

Online Security and Website Data

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 to identify unauthorised attempts to upload or change information, or otherwise cause us damage.

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.

Notification of 'Eligible Data Breaches' and loss of Personal Information

> 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 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 primary categories, serious (eligible) and minor. To ensure breaches are promptly responded to, we will implement a Data Breach Response Plan. Minor breaches are those that are rectified quickly and individuals are not at risk of suffering serious harm.

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

- if the breach is significant (i.e. eligible), immediately notify the Privacy Commissioner (at the Office of the Australian Information Commissioner - OAIC).
- 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

Complaints about Privacy Breaches

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 procedures and policy on Monitoring Quality and Performance.

We will ensure that our work is supported by integrated, efficient and secure information technology and infrastructure. We maintain and regularly update a computer system to provide staff with reliable software, high speed internet access and email and messaging systems. All client data is stored in Australia. Where possible and or required by Australian law, cloud-based data is also stored in Australia. We will manage our information effectively and maintain associated procedures including continuity and recovery plans for accidental loss of data or information.

We recognise that an important part of effective information management is the provision of an accessible and efficient reception and messaging service. We will maintain central administration to provide reception services for people contacting us and related message / information handling.

Social Futures will recognise and protect intellectual property (IP) rights in accordance with copyright law and ethical considerations. We aim to protect both our own IP rights and the rights of others in any material produced by us or on our behalf. All staff, Board members, volunteers and contractors must observe applicable laws and regulations in producing / using our material.

*The Federal Privacy Act does not apply to employee records for current and former staff if the records are *only* used for purposes that are directly related to the employment relationship. If they're used for other purposes, the Act *does apply*. Records about prospective employees who don't become employees and records about volunteers must be handled in compliance with the Act.

Policy Administration

Policy context: This policy relates to	
Standards or other external requirements	Australian Service Excellence Standards C.2.2, 2.3 Family Relationships Services Standards 12 National Home Care Standards 3.2 National Standards for Mental Health Services 1.8 Rainbow Tick 5.2
Legislation or other requirements	Australian Charities and Not for Profits Commission Act 2012 (Clth) Corporations Act 2001 (Clth) Children and Young Person Care and Protection Act, 1998 Freedom of Information Act 1989 (NSW) Financial Management and Accountability Act 1997 (Clth) Health Records and Information Privacy Act 2002 (NSW) Information Privacy Act 2009 (Qld) Privacy Act 1988 (Clth) Privacy and Personal Information Protection Act 1998 (NSW)

Reviewing and approving this policy		
Frequency	**Person responsible**	**Approval**
Yearly	Chief Executive Officer	Board

Policy review and version tracking				
Review	**Date Approved**	**Document Reviewed**	**Approved by**	**Next Review Due**
1a	30/01/2020	Privacy	Board	Reviewed 23/6/2021 as one merged policy Privacy, Information and Knowledge Management
1b	30/01/2020	Information and Knowledge Management	Board	
	28/07/2021	Privacy Information and Knowledge Management	Board	23/09/2022
	4/10/2022	Privacy Information and Knowledge Management	Board	4/10/2023

Documentation

Documents related to this policy	
Related policies	Compliance and Risk Management Employment, Equity and Diversity Monitoring Quality and Performance Workplace Management
Related procedures	Data Breach Response Plan Practice Framework Risk Management Framework