POLICY

Safety, Wellbeing & Rights

Contents

Revision History

Revision	Details	Date Released
1	Release under new format. Was MA-009	31-Mar-2015
2	Internal privacy, database and security restrictions	18-Nov-2015
3	Board Review - Verification of Identity added; Notification of Firearm amended to include Weapons; Reference to single confidentiality agreement form; Data security personnel updated	27-July-2016
4	Responding to Subpoena added; Evidence Act added to legislation; Letter of Objection added to related docs.	11-Jan-17
5	Privacy Act amendments included	20-Sep-2018
6	Minor review; new format.	4-Oct-2019
7	Minor review; SA requirements in disclosure added; subpoena process updated; legislation updated.	27-May-2020
8	Minor review; COVID-19 notification added.	24-June-2020

Applicable Legislation and Standards

ISO9001 Quality Management System
Human Services Quality Framework
Child Protection Act 1999 (QLD)
Child Protection Reform Amendment Act 2017 (QLD)
Child Protection (working with children) Act 2012 No 51 (NSW)
Evidence Act 1929 SA
Evidence Act 1995 NSW
Evidence Act 1997 QLD
Firearms Act 1977 (SA)
Human Rights Bill 2019 (Qld)
Privacy Act 1988
Privacy Amendment (Enhancing Privacy Protection) Act 2012
Privacy Amendment (Notifiable Data Breaches) Act 2017
South Australian Children and Young People (Safety) Act 2017

Links to other Related Documents

Doc No.	Title	Doc No.	Title
FCA-07	Feedback, Complaints and Appeals	ICN-05	Responding to Individual & Community Needs
PRO-0101	Group Organisational Structure	PRO-0701	Feedback
PRO-0702	Complaints	PRO-0703	Appeals
F05.06	Client's Privacy and Disclosure Form	F06.01	Letter of Objection to Subpoena
F07.02	Client Complaint Form	PD486A	Medical notification to the Registrar of Firearms

Purpose

The purpose of this policy is to state the rights of clients of services to receive services of the organisation in a way that ensures safety and wellbeing.

Background

The Drug Awareness and Relief Foundation (Australia) (DARFA) is the parent company of all subsidiary companies (refer **PRO-0101 Group Organisational Structure**). Collectively these entities are referred to as the Group.

DARFA provides overarching governance of the Group. Subsidiary Boards meet annually and report to the DARFA Board.

For the purpose of this document:

(i) the Board refers to the DARFA Board;
(ii) the Committee refers to DARFA appointed Committees;
(iii) the Organisation refers to the individual entities of the DARFA group.

Scope

This document applies to all staff and volunteers of the organisation as well as any external contractors who have entered into an agreement with the organisation

Compliance

Depending on the circumstances, non-compliance with this policy may constitute a breach of contract of employment or other contractual obligations, misconduct, sexual harassment, discrimination, or some other contravention of the law.

Failure to comply with the policy may therefore result in disciplinary action and, in more serious cases, may result in termination of employment.

Definitions

Online users refers to anyone that accesses any the organisation's website/s.

Personal information as defined by the Privacy Act 1988 (as amended) is information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether true or not, and whether recorded in a material form or not.

Sensitive information as defined by the Privacy Act 1988 (as amended) is information or opinion (that is also personal information) about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices or criminal record or health, genetic, biometric information or biometric templates, that is also personal information.

The website means any of the website/s of the organisation.

Policy

Privacy

The organisation respects the privacy of all stakeholders of the organisation including members, employees, volunteers, our clients/beneficiaries, donors, business partners, and online users. The organisation is committed to safeguarding all personal information that is provided to the organisation during its interactions.

The organisation is committed to complying with the Privacy Amendment (Private Sector) Act 2000, Privacy Amendment (Enhancing Privacy Protection) Act 2012, Privacy Amendment (Notifiable Data Breaches) Act 2017, and the privacy provisions of all applicable legislation.

The Acts set clear standards for the collection, access, storage, use and breach of personal information that we obtain as part of our business operations and service provision. This includes information we have collected from people in person, via email, from our website, over the phone and on work sites. Work sites include sites not considered premises of the organisation where the organisation's business is conducted or services provided.

Purpose

The purpose of this privacy policy is to:

- Clearly communicate the personal information handling practices of Drug ARM
- Enhance the transparency of the organisation's operations, and
- Give individuals a better and more complete understanding of the sort of personal information that the organisation holds, and the way we handle that information.

Information Collected

Only information that is considered necessary; through Government and funding body requirements, service provision requirements or the organisation will be collected.

Information that is given to the organisation will be used in the manner that is stipulated when the information is given. No information will be given to a third party without written consent of the individual who provided the information except in exceptional circumstances. Information will only be given to a third party without written consent, when in compliance with request of law enforcement or government departments. No information gathered including names, e-mail addresses or phone numbers will be sold to a third party. De-identified data may be collected for use in reports to funding bodies, research and marketing promotions.

Personal information may be used in:

- Administering the individual's employment and/or contract;
- For insurance purposes;
- To satisfy the legal obligations of the organisation.

All staff, volunteers, students and contractors of the organisation sign a Confidentiality Agreement form and are aware of procedures to ensure the safety of information. Clients are made aware of how to make a complaint to Government department.

Client Information

The organisation collects information from clients to inform the services it provides, to monitor changes in clients across time, to report general statistics and trends to funding bodies and interested parties.

Health and welfare information collected may include, but is not limited to:

- An individual's personal information e.g. address, phone number etc.;
- An individual's health or ability at any time past, present or future;
- An individual's expressed wishes regarding future health service;
- Health services provided, or to be provided, to the individual.

The organisation may collect personal information about:

- Clients and their families (significant others) before, during and after the client has received services and support.

Clients are made aware of the collection and use of their information at the first client session.

Student Information

Reasonable care is taken to protect all information that is collected relating to student's training as well as personal information from misuse, loss, unauthorised access, modification or disclosure including restricted access to electronic files, secure storage of paper files and back up of data.

Marketing and Fundraising Information

The organisation may gather information from donors, potential donors and support members for the purpose of marketing and fundraising. Personal information held by the organisation may be disclosed confidentially to an organisation that assists the organisation in fundraising activities as authorised by the Executive Director.

As per National Privacy Principle No 2 Use and Disclosure – 2.1(c) if the information is not sensitive information and the use of the information is for the secondary purpose of direct marketing:

- it is impracticable for the organisation to seek the individual's consent before that particular use; and
- the organisation will not charge the individual for giving effect to a request by the individual to the organisation not to receive direct marketing communications; and
- the individual has not made a request to the organisation not to receive direct marketing communications; and
- in each direct marketing communication with the individual, the organisation draws to the individual's attention, or prominently displays a notice, that he or she may express a wish not to receive any further direct marketing communications; and
- each written direct marketing communication by the organisation with the individual (up to and including the communication that involves the use) sets out the organisation's business address and telephone number and, if the communication with the individual is made by fax, telex or other electronic means, a number or address at which the organisation can be directly contacted electronically.

Permission must be obtained from the Executive Director before any donor information is downloaded or transferred via electronic format.

Disclosure of Clients' Information

Information may be disclosed in the following circumstances with written permission from the client:

- To another agency, for the purpose of referral or case conferencing;
- Government departments;
- Medical practitioners;
- People providing services to the organisation, including specialist medical and allied health professional;
- Anyone that the individual/ client authorises

Information may be disclosed without permission from the client as per National Privacy Principles No 2 Use and Disclosure – 2.1(e) "the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent" in the following circumstances:

- a serious and imminent threat to an individual's life, health or safety; or
- a serious threat to public health or public safety.
- And 2.1 (g)
- The use or disclosure is required or authorised through subpoena[1] or under law.

Under Section 150 of the South Australian Children and Young People (Safety) Act 2017, the organisation must provide information and documentation if requested by notice in writing by a Child Protection Officer in South Australia.

[1] Subpoena requests differ in each state. Check validity of request against the relevant statutory process.

Verification of identity

Before any personal information is disclosed, staff will assure themselves of the identity of the requestor. This will be done at the discretion of the staff member to a reasonable level, and can be through sighting a photo identification (ID). Staff receiving an enquiry from a member of the community in person, by telephone, fax or by email will undertake verification process with the individual and assure themselves of their identity, before any personal information related to the individual is disclosed.

Where possible, requests for personal information will be made in writing and received through the organisation's mail or email system. Requests for personal information will be in writing and be supported by the requestor's authority to seek information. This authority will be sighted before any personal information is disclosed.

Database Security and Privacy

The organisation utilises a CRM database to manage all client information. The following guidelines are to be strictly adhered to by all staff to ensure privacy and other legislative requirements are complied with:

- Only staff responsible for a client are to access the relevant client files and database information
- Staff are not to discuss client information amongst other clinicians
- Staff are not to share security passwords and log in details with others
- With the exception of formal meetings amongst clinicians internally on clients, for learning purposes only, clients are to be allocated a separate identifier and are not to be identified by their name.

Any breaches of the above guidelines will be reported to management and viewed as serious misconduct which may result in disciplinary action.

Disclosure of Student Information

Student information may be used by State and Federal government agencies for statistical, reporting and or funding purposes. Students' private or personal information will not be disclosed or used in any way other than the purposes stated without their consent unless required by law.

Access to the Client/Individual's own Information

The client/ individual will have access to any of their personal information that the organisation holds, except in circumstances where another person's privacy may be compromised if the information is disclosed and other circumstances recognised by privacy law.

Further Privacy Information

More information about Privacy law and the National Privacy Principles is available from the Federal Privacy Commissioner at *http://www.privacy.gov.au*

Related policy and procedures include:

- Privacy and Confidentiality Agreement
- Client Disclosure Form
- Programs Policy and Procedure
- Treatment Process
- Filing, Records and Archiving (includes retention periods)

Review and Enquiries

This policy will be reviewed at least annually and any amendments will be incorporated in the updated policy.

Outline of this policy

'Part A – Personal Information Handling Practices' explains our general information handling practices across the organisation including information about how we collect, use, disclose and store your personal information.

'Part B – Files' offers further detail by explaining our personal information handling practices in relation to specific organisation functions or activities such as client files, and student and volunteer records. Here you can find out what sort of records we keep and why.

Part A – Personal Information Handling Practices

Our obligations under the Privacy Act

This privacy policy sets out how we comply with our obligations under the Privacy Act 1988 (Privacy Act). We are bound by the Australian Privacy Principles (APPs) in the Privacy Act which regulate how organisations may collect, use, disclose and store personal information, and how individuals may access and correct personal information held about them.

Collection of personal and sensitive information

If you would like to access any of the organisation's services on an anonymous basis or using a pseudonym, please tell us. If this is possible and lawful, we will take all reasonable steps to comply with your request. However, we may not be able to provide the services in question if we are not provided with the personal information requested.

The nature and extent of personal and sensitive information collected by the organisation varies depending on your particular interaction with the organisation.

The organisation collects personal and sensitive information from clients/beneficiaries, donors, business partners, staff and volunteers of the organisation, and online users. Further information about the kind of information collected from each of these groups and the usage of such information is detailed below.

Clients and Beneficiaries

Type of information collected:

- Contact details (name, address, email, etc.)
- Personal details including: date of birth, gender, income
- Information on personal issues and experiences, relationships
- Family background, supports clients may have in the community
- Areas of interest
- Health information and/or medical history
- Credit card numbers or bank account details

How the information is collected:

- Initial contact including eligibility screen
- Initial assessment
- Online registration
- Sessions
- Application/enrolment forms
- Telephone

Purpose for which the organisation uses the information:

- To provide services
- To provide clients/beneficiaries with the most appropriate services for their needs
- To meet any requirements of government funding for programs
- To monitor and evaluate existing services and plan for future services
- To produce annual reports and for research purposes that may involve contracted organisations
- To comply with legal obligations

Donors

Type of information collected:

- Contact details (name, address, email, etc.)
- Personal details including: date of birth, gender, income

- Areas of interest
- Donation history
- Credit card numbers or bank account details of all our donors
- Expiration date of credit card

How the information is collected:

- Communications, email, flyers
- Online registration
- Telephone

Purpose for which the organisation uses the information:

- To provide services
- To process donations and provide accurate receipts
- To facilitate on-going fundraising and marketing activities
- To comply with legal obligations
- To provide transparency relating to donated funds, particularly for Appeals for public donations

Business Partners

Type of information collected:

- Contact person's name, the name of the organisation which employs the person, telephone numbers, fax number, street and postal address, email address and position title
- Areas of interest by category and industry
- Bank details (if the organisation is to receive payment or make payment for services received)
- Australian Business Number (ABN)
- Type of support (e.g. Workplace giving, goods in kind, program support, volunteering)

How the information is collected:

- Communications, email, flyers
- Online registration
- Telephone

Purpose for which the organisation uses the information:

- To provide services
- To process donations and provide accurate receipts
- To pay for services

- To establish and manage partnerships
- To receive services from you or the organisation that employs you
- To manage the organisation's relationship with the business partner
- To provide information about the organisation's services
- To update the company on the organisation's appeals for public donations, programs and services

People (volunteers, employees, delegates) and candidates for volunteer work and prospective employees)

Type of information collected:

- Contact details (name, address, telephone numbers, email, etc.)
- Personal details including personal details of emergency contact person(s)
- Date of birth
- Country of birth, citizenship, residency and/or visa details
- Details of current/previous employment or volunteer involvement
- Skills and experience
- Languages spoken and written
- Qualifications, drivers licence details
- Information and opinions from referees for prospective employees and candidates for volunteer work
- A police check may be required for some roles in the organisation (particularly those involving children, young people and other vulnerable individuals). Individuals will be required to provide certain information for a Police Check. There are different arrangements for Police Checks in each state and territory of Australia. In some cases, the Police Check will be received directly by the organisation and then stored securely or destroyed.
- In some situations, it is necessary for the organisation to collect or receive information about an individual's health. In this circumstance, the organisation will advise why the information is being collected and whether and to whom it will be released.

Purpose for which the organisation uses the information:

- To provide services
- To process an application to become a member, volunteer or employee of our organisation
- To facilitate a placement in an appropriate service or position
- To assist with services whilst an individual is employed or engaged as a volunteer with the organisation
- To provide feedback on performance as a volunteer or employee
- To meet legislative responsibilities to all volunteers and employees
- To obtain feedback from individuals about their experiences

- To assist the organisation to review and improve its programs and services to keep individuals informed about the organisation's developments and opportunities
- To provide information about the organisation's services
- To facilitate further involvements with the organisation (e.g. membership, donor)

Members

Type of information collected:

- Contact details (name, address, telephone numbers, email, etc.)
- Date of birth
- Credit card details
- Expiration date of credit card
- Areas of interest

Purpose for which the organisation uses the information:

- To provide services
- To provide communication updates and ensure transparency relating to donated funds, particularly Appeals for public donations, and organisation operations
- To process donations and provide accurate receipts
- To facilitate ongoing fundraising and marketing activities
- To provide information about the organisation
- To receive invitations to upcoming events and activities
- To recognise your support of the organisation

Online Users

To the extent that this Privacy Policy applies to online privacy issues, it is to be read as forming part of the terms and conditions of use for the organisation's website.

Type of information collected:

- Contact details (name, address, telephone numbers, email, etc.)
- Credit card number
- Expiration date of credit card
- Non-personal information e.g. Visitor navigation and statistics
- Server address, browser type, date and time of visit
- Personal information

Purpose for which the organisation uses the information:

- To process donations, purchase orders, online bookings, purchases/transactions (e.g. Booking First Aid Health & Safety courses)
- To analyse website usage and make improvements to the website
- The organisation does not match the personal information collected with the non-personal information.

Additional information

The website may from time to time contain links to other websites. The organisation stresses that when an online user accesses a website that is not the organisation's website, it may have a different privacy policy. To verify how that website collects and uses information, the user should check that particular website's policy.

How we collect information

Where possible, we collect your personal and sensitive information directly from you. We collect information through various means, including telephone and in-person interviews, appointments, forms and questionnaires. If you feel that the information that we are requesting, either on our forms or in our discussions with you, is not information that you wish to provide, please feel free to raise this with us.

In some situations, we may also obtain personal information about you from a third party source. If we collect information about you in this way, we will take reasonable steps to contact you and ensure that you are aware of the purposes for which we are collecting your personal information and the organisations to which we may disclose your information, subject to any exceptions under the Act. For example, we may collect information about you from a health care professional, such as your doctor.

Health Information

As part of administering the organisation's services, the organisation may collect health information. For example, the organisation collects health information (such as medical history) from some clients/beneficiaries participating in organisation programs. When collecting health information from you, the organisation will obtain your consent to such collection and explain how the information will be used and disclosed.

If health information is collected from a third party (such as your doctor), the organisation will inform you that this information has been collected and will explain how this information will be used and disclosed.

The organisation will not use health information beyond the consent provided by you, unless your further consent is obtained or in accordance with one of the exceptions under the Privacy Act or in compliance with another law. If the organisation uses your health information for research or statistical purposes, it will be de-identified if practicable to do so.

Use and disclosure of Personal Information

We only use personal information for the purposes for which it was given to us, or for purposes that are related to one of our functions or activities.

For the purposes referred to in this Privacy Policy (discussed above under 'Collection of Personal and Sensitive Information'), we may also disclose your personal information to other external organisations including:

- Government departments/agencies who provide funding
- Contractors who manage some of the services we offer to you, such as distribution centres that may send information to you on behalf of the organisation. Steps are taken to ensure they comply with the APPs when they handle personal information and are authorised only to use personal information in order to provide the services or to perform the functions required by the organisation
- Doctors and health care professionals, who assist us to deliver our services
- Other regulatory bodies, such as WorkSafe
- Referees and former employers of the organisations employees and volunteers, and candidates for the organisation employee and volunteer positions, and
- Our professional advisors, including our accountants, auditors and lawyers.

Except as set out above, the organisation will not disclose an individual's personal information to a third party unless one of the following applies:

- The individual has consented
- The individual would reasonably expect us to use or give that information for another purpose related to the purpose for which it was collected (or in the case of sensitive information – directly related to the purpose for which it was collected)
- It is otherwise required or authorised by law
- It will prevent or lessen a serious threat to somebody's life, health or safety or to public health or safety
- It is reasonably necessary for us to take appropriate action in relation to suspected unlawful activity, or misconduct of a serious nature that relates to our functions or activities
- It is reasonably necessary to assist in locating a missing person
- It is reasonably necessary to establish, exercise or defend a claim at law
- It is reasonably necessary for a confidential dispute resolution process
- It is necessary to provide a health service
- It is necessary for the management, funding or monitoring of a health service relevant to public health or public safety
- It is necessary for research or the compilation or analysis of statistics relevant to public health or public safety

- It is reasonably necessary for the enforcement of a law conducted by an enforcement body.

The organisation does not usually send personal information out of Australia. If we are otherwise required to send information overseas we will take measures to protect your personal information. We will protect your personal information either by ensuring that the country of destination has similar protections in relation to privacy or that we enter into contractual arrangements with the recipient of your personal information that safeguards your privacy.

Any breaches of protection of personal information relating to clients accessing the programs must be reported to the relevant funding body.

Security of Personal and Sensitive Information

Drug ARM takes reasonable steps to protect the personal and sensitive information we hold against misuse, interference, loss, unauthorised access, modification and disclosure.

These steps include password protection for accessing our electronic IT system, securing paper files in locked cabinets and physical access restrictions. Only authorised personnel are permitted to access these details.

When the personal information is no longer required, it is destroyed in a secure manner, or deleted according to our File, Records & Archiving Management Policy.

Access to and Correction of Personal Information

If an individual requests access to the personal information we hold about them, or requests that we change that personal information, we will allow access or make the changes unless we consider that there is a sound reason under the Privacy Act or other relevant law to withhold the information, or not make the changes.

Requests for access and/or correction should be made to the Privacy Officer (details of which are set out below). For security reasons, you will be required to put your request in writing and provide proof of your identity. This is necessary to ensure that personal information is provided only to the correct individuals and that the privacy of others is not undermined.

In the first instance, the organisation will generally provide a summary of the information held about the individual. It will be assumed (unless told otherwise) that the request relates to current records. These current records will include personal information which is included in the organisation's databases and in paper files, and which may be used on a day to day basis.

We will provide access by allowing you to inspect, take notes or print outs of personal information that we hold about you. If personal information (for example, your name and address details) is duplicated across different databases, the organisation will generally provide one printout of this information, rather than multiple printouts.

We will take all reasonable steps to provide access or the information requested within 14 days of your request. In situations where the request is complicated or

requires access to a large volume of information, we will take all reasonable steps to provide access to the information requested within 30 days.

The organisation may charge you reasonable fees to reimburse us for the cost we incur relating to your request for access to information, including in relation to photocopying and delivery cost of information stored off site. For current fees, please contact the Privacy Officer.

If an individual is able to establish that personal information the organisation holds about them is not accurate, complete or up to date, the organisation will take reasonable steps to correct our records.

Access will be denied if:

- The request does not relate to the personal information of the person making the request
- Providing access would pose a serious threat to the life, health or safety of a person or to public health or public safety
- Providing access would create an unreasonable impact on the privacy of others
- The request is frivolous and vexatious
- The request relates to existing or anticipated legal proceedings
- Providing access would prejudice negotiations with the individual making the request
- Access would be unlawful
- Denial of access is authorised or required by law
- Access would prejudice law enforcement activities
- Access would prejudice an action in relation to suspected unlawful activity, or misconduct of a serious nature relating to the functions or activities of the organisation
- Access discloses a 'commercially sensitive' decision making process or information, or
- Any other reason that is provided for in the APPs or in the Privacy Act.

If we deny access to information we will set our reasons for denying access. Where there is a dispute about your right of access to information or forms of access, this will be dealt with in accordance with the complaints procedure set out below.

Changes to this Privacy Policy

The organisation reserves the right to review, amend and/or update this policy from time to time.

We aim to comply with the APPs and other privacy requirements required to be observed under State or Commonwealth Government contracts.

If further privacy legislation and/or self-regulatory codes are introduced or our Privacy Policy is updated, we will summarise and substantial modifications or enhancements in this section of our Privacy Policy.

Part B – Files: how we handle specific types of files that contain personal information

Public Awareness and Education Files

Public awareness and education files record details of public awareness and educational activities, such as contact with the media, speeches, event management, surveys and publication preparation.

The limited personal information in public awareness and education files relates to organisations, individuals, media representatives, event attendees, service providers and events calendar listings that appear on our website.

Collection

It is our usual practice to collect personal information in public awareness and education files directly from individuals.

Sometimes we may collect personal information from an individual's representative or from publicly available sources such as websites or telephone directories.

Use and Disclosure

We only use the personal information in public awareness and education files for the purposes of undertaking public awareness and education initiatives and managing public relations.

The personal information on public awareness and education files is not disclosed to other organisations or anyone else without consent unless the individual would reasonably expect, or has been told, that information of that kind is usually passed to those organisations or individuals, or the disclosure is otherwise required or authorised by law.

Data Quality

We maintain and update personal information in our public awareness and education files as necessary, or when we are advised by individuals that their personal information has changed.

Data Security

Public awareness and education files are stored in either password protected electronic media or in locked cabinets in paper form. When no longer required, personal information in public awareness and education files is destroyed in a secure manner or deleted in accordance with our File, Records & Archiving Management Policy.

The following staff members have access to public awareness and education files on a need to know basis:

- Directors
- Policy staff
- Corporate Services staff
- Executive and Senior Management

Access and Correction

For information about how to access or correct personal information in public awareness and education files, see '**Access and Correction**' in **Part A** of this document.

Contacts Lists

Purpose

We maintain contacts lists which include contact information about individuals who may have an interest in disability services. We use these contact lists to distribute information about our activities and publications.

Collection

It is our usual practice to collect personal information in contacts lists directly from individuals, for example, where they have asked to be added to a contact list.

Sometimes we collect personal information from a third party or from a publicly available source such as a website or telephone directory. We usually only collect personal information in this way if the individual would reasonably expect us to, or has given their consent. For instance, we might collect this information if we thought that the individual (or the organisation that they work for) would like to receive information about services we are carrying out, or that they might be likely to consider information about our services useful in the work they do. We would only contact this individual in their work capacity.

Use and Disclosure

We only use personal information in contacts lists for the purpose of managing stakeholder relations.

We do not give personal information about an individual to other organisations or anyone else without consent unless the individual would reasonably expect, or has been told, that information of that kind is usually passed to those organisations or individuals, or the disclosure is otherwise required or authorised by law.

Data Quality

We maintain and update personal information in our contacts lists when we are advised by individuals that their personal information has changed. We also

regularly audit contacts lists to check the currency of the contact information. We will remove contact information of individuals who advise us that they no longer wish to be contacted.

Data Security

The personal information in the contacts lists is stored in either password protected electronic media or in locked cabinets in paper form. When no longer required, personal information in contacts lists is destroyed in a secure manner or deleted in accordance with File, Records & Archiving Management Policy.

Routine access to contacts lists is limited to the database operators who have responsibility for maintaining the contacts lists. Other staff members have access to the personal information in contacts lists on a need to know basis.

Access and Correction

For information about how to access or correct personal information in public awareness and education files, see '**Access and Correction**' in **Part A** of this document.

Responding to a Subpoena

Subpoenas are managed centrally by a member of the management team. The management team must be notified of a subpoena request.

Subpoenas will most likely be requested by a Solicitor but issued by the Courts:

- QLD – Supreme Court or District Court of Queensland
- NSW – Supreme Court; District Court; Police Officers and a Prosecutor who is a Public Officer (being council employees, officer or employee of a statutory body representing the Crown, Director of Public Prosecutions etc); Local Court proceedings
- SA – Deputy Registrar of the Supreme Court of South Australia and includes any officer of the Court assigned by the Chief Justice

1. Preparing subpoenaed files

Carefully read over what is being requested in the subpoena and the timeframe associated. You can contact the solicitor stated on the subpoena to clarify what is being requested if you have questions. Ensure that when you contact the solicitor you maintain the client's confidentiality, only ask general questions around what is required, do not offer details contained in the client's file.

Contact your direct supervisor/line manager and let them know you have files that have been subpoenaed. They will seek confirmation from the Executive Director or nominee that the request is a legally binding subpoena. Your manager will then work to support you in ensuring you have time to prepare the files.

The subpoena may ask for originals, but generally it will ask for a copy. If you are unsure, you can contact the court registrar on the subpoena. Paper files should be photocopied. Files from the database can be printed or saved on a CD. All

subpoenaed documents should be placed in an envelope together. When working on preparing the subpoenaed documents the utmost care should be taken to ensure privacy and confidentiality of the files; ensure materials are stored like hardcopy case files (i.e. in locked drawers) when not being worked on.

You MUST NOT amend or change the content of your case notes once receiving a subpoena. The reality is that your case files can be subpoenaed at any time and this is one of many reasons that the utmost care and professionalism should be used in client file documentation. You can make objections about the case files being used in the court proceedings, see "Objections" below.

You must deliver, or arrange the delivery of, the subpoenaed documents to an adult at the address stated on the subpoena.

Copies of the Subpoena and detailed case notes should be made in the clients file.

2. Objections

You MUST supply the requested information to the court, however you can make an objection to all or some of the material being used. Objections may be based on the information putting the health or safety of the client, or another person, at risk; information that is not relevant to the proceedings and is sensitive; or other scenarios where the release of the information may be harmful. Refer **Objection to Subpoena Letter** (**F06.01**)

The process may vary across courts, so contact the court for details. Generally, you will supply a written objection, and in a separate envelope supply all subpoenaed documents highlighting or noting the items you object to.

If you do not have the grounds for an objection you may identify certain materials as "sensitive" and request that the Judge or Magistrate reviews the information to decide on the limitations they will set around disclosure.

If you are considering an objection discuss this with your manager so that the organisation can support you in preparing the documentation.

You MUST supply all subpoenaed documents. Withholding documentation, even on the grounds of professional discretion, may place you in contempt of court and have legal consequences.

3. Notifying clients

It is best practice to notify the client that their files have been subpoenaed. Be clear that you are contacting them as a courtesy and not for their consent. Explain that you are legally obligated to supply the information. You can remind them of how this was covered in the Privacy and Confidentiality Agreement at the start of their engagement with the service. You may state any objections you made to the court about the files being used, but be clear that the court may choose to ignore these objections.

4. Requesting reimbursement for the preparation of materials

In most cases you can request reimbursement through the court for time and materials used to prepare the subpoenaed files. Discuss with your manager whether this will be a process you will undertake. For many simple requests this will be

unnecessary, but when large amounts are requested, or items are recalled from archives, this process may help recover costs for the organisation. The amount covered varies between courts and should be investigated. Record time spent and cost at your hourly rate, for photocopied materials cost at $0.50/page, if a CD is supplied cost the price of the CD, if items are recalled from archives include the cost from the archiving company. Contact the finance department for the preparation of an invoice.

Where a cheque or payment accompanies the subpoena, discuss with your supervisor/line manager if the amount is adequate and forward to Corporate Services for processing.

5. Questions or concerns

If you have any questions about what information is being requested, you can contact the *solicitor requesting the case files.*

If you have any questions about how to submit the files (format, originals, etc.), how to make an objection or identify material as sensitive (i.e. requesting the Judge consider what is relevant and what should be disclosed), or how to reclaim cost associated with preparing the subpoenaed files, contact *the court that issued the subpoena.*

If you have any other questions you can talk to your manager. If necessary, the organisation can seek legal advice.

Child Safe Environments

This policy represents a strong commitment to child safety and to maintaining child safe environments within all programs and services. The organisation recognises that every person engaged with our organisation has the right to an environment free from abuse.

This policy complies with our obligations under the Children and Young People (Safety) Act 2017 (SA), the Child Protection Act 1999 (Qld), the Child Protection Reform Amendment Act 2017 (QLD), and the Child Protection (working with children) Act 2012 No 51 (NSW).

All children who are involved with one of the organisations, either as a client or the child in the care of a client have a right to feel and be safe. We are committed to the safety and well-being of all children and young people accessing our services, and the welfare of the children in the care of clients is our first priority. This commitment is demonstrated in the following ways:

- We aim to create a child safe environment where all children feel valued and safe.
- We encourage children who use our services to express what is important to them.
- We value diversity and do not tolerate any discriminatory practices, harassment or bullying (refer to **ACC-04 Service Access**).

- We listen to and act on concerns that children, or their parents, raise with us (refer to **FCA-07 Feedback, Complaints and Appeals**).
- We apply best practice standards in the screening and recruitment of employees and volunteers.
- We conduct a criminal history assessment for all employees and volunteers and ensure that criminal history information is dealt with in accordance with best practice standards (refer to **HRE-08 Human Resources**).
- We comply with the Privacy Act 1988 (including amendments) in all of our dealings with children and any records relating to their involvement with our organisation. Refer to the section **'Privacy'** in this policy document.
- All employees and volunteers are made aware of and must abide by our Code of Conduct (refer to **HRE-08 Human Resources**).
- We seek to attract and retain a high standard of employees and volunteers who are provided opportunities for regular supervision, support, training and professional development (refer to **HRE-08 Human Resources**).
- We carry out regular risk assessments relating to the maintaining of child safe environments within the organisation (refer to **PRO-0213 Risk Management**).

The organisation will not tolerate incidents of child abuse. All employees and volunteers understand their obligation to notify the relevant state authority as soon as practicable if they have a reasonable suspicion that a child has been, or is being, abused or neglected. We ensure that employees and volunteers are aware of how to make appropriate reports and provide opportunities for staff and volunteers to attend Child Safe Environment training.

Employees and volunteers must also report to management any reasonable suspicion that a child has been, or is being abused or neglected by another employee or volunteer. The organisation may resolve to take protective action to keep the child and others safe.

Notification of Firearms and Weapons

Should an employee of the organisation suspect that:

- A client is suffering from a physical or mental illness or condition, **and**
- there is a threat to the person's safety or the safety of another person, **and**
- there is a risk associated with the person's possession or use of a firearm or other weapons,

they should make a report to their state police of this suspicion as soon as possible after first becoming suspicious. Employees and volunteers must report the incident to management and file an incident report as soon as possible.

(South Australia only)

Where the weapon is a Firearm, complete the Medical Notification to the Registrar of Firearms online form (PD486A). Submit the form by pressing email. A copy should be kept in the appropriate client file. Employees and volunteers must report the incident to management and file an incident report as soon as possible.

https://www.police.sa.gov.au/__data/assets/pdf_file/0016/2590/medical_notification_to_registrar_pd486a.pdf

Reporting

The Executive Director will report against this policy to the board through the Risk and Compliance Committee.

Review

The policy will be reviewed every three (3) years, or as directed by the board, by the Risk and Compliance Committee who will recommend the reviewed policy for approval to the board.