Privacy and Confidentiality Policy.

Contact Officer:	Office Manager	
Consultation:	All Staff	
Internal Approval:	CEO – 25/01/2022	
Final Approval:	Board – 25/01/2022	
Next Review Date:	January 2023	
Quality Improvement Council Standards Alignment:	Standard 1.6	Risk is identified, assessed and controlled across the whole organisation.
	Standard 2.2	Human resources are managed to ensure and effective and competent service.
	Standard 2.3	Information held by the organisation is accurate, secure and accessible.
Legislation and Guidelines:	• *Privacy Act 1988* (Cth) • *Privacy and Personal Information Act 1998* (NSW) • *Health Records and Information Privacy Act 2002* (NSW) • *State Records Act 1998* (NSW) • *General Retention and Disposal Authority - Public Health Services: Patient/Client records (GDA17)* • *Workplace Surveillance Act 2005* (NSW)	
Related Policies/ Attachments/ Forms:	**2.7 Complaints and Compliments Policy** **4.4 Code of Ethics** **6.1 Counselling Service Policy Manual** **6.2 Counselling Quality Management Policy Manual**	

	Best Practice Manual for Specialised Sexual, Domestic and Family Violence Counselling 2.5a Data breach response plan 2.5b Storage and security procedures

Contents

1 Principles

1.1 All personal, sensitive and health information provided to Full Stop Australia (FSA) by clients, staff, board, ambassadors, volunteers, students, supporters and donors will be managed in accordance with this policy.

1.2 FSA will take all reasonable security safeguards to protect against unauthorised use, disclosure, loss or other misuse of information.

2 Client Information

2.1 Principles of client confidentiality

2.1.1 FSA recognises the critical importance of client confidentiality to providing high quality, trauma responsive and client-centered counselling services to people who have been impacted by sexual, domestic and family violence. These crimes constitute a

fundamental violation of trust and it is essential that this dynamic is not replicated. FSA is committed to providing services in an ethical way that creates opportunities for clients to rebuild a sense of control and empowerment and maintains client confidentiality and privacy wherever possible.

2.1.2 Staff will always seek to safeguard the confidentiality of client information, except in circumstances where:

- There is a serious and immediate risk of harm to the client or another person;
- The client has provided informed consent to disclose information to a third party;
- The client discloses that they have perpetrated sexual, domestic or family violence and provides information that may assist in a current criminal investigation or prosecution;
- The organisation has a legal obligation to disclose client information.

2.1.3 Staff recognise that where client confidentiality is compromised this may have negative impacts including:

- The client feeling violated or betrayed;
- The client experiencing a heightened sense of shame, guilt, fear or disconnection from community;
- Damage to the therapeutic relationship and trust between counsellor and client and therapeutic outcomes;
- A risk of further harm to the client, where an offender obtains access to personal or sensitive information about the client;
- Reduced willingness by the client and others to report sexual, domestic or family violence to service providers.
- Reduced willingness to engage with therapeutic or health services of any kind in the future.

2.1.4 FSA will always treat client information in accordance with professional codes of ethics published by the Australian Psychological Society (APS), Australian Association of Social Workers (AASW) and the Counsellors and Psychotherapists Association (CAPA).

2.2 Informed consent

2.2.1 FSA will always seek informed, voluntary, current and specific consent from a client before collecting, recording, using or disclosing any sensitive information. This includes that the client has experienced sexual, domestic or family violence.

2.3 Purpose and use of collecting client information

2.3.1 FSA collects client information for the following purposes:

- To inform quality counselling service provision;
- To establish and review therapeutic plans and clinical care networks;
- To communicate with emergency or support services where the organisation identifies a duty of care to a client or another person at risk of harm;
- To prepare reports at the request of the client or at the request of a third party with the client's consent;
- To submit a claim for assistance to a third party at the request of the client;
- To prepare a response to a complaint; and
- To prepare reports containing non-identifying statistical information to the Board, funding bodies, stakeholders, or other interested individuals and bodies. The purpose of these reports is for transparency in relation to services provided, quality improvement and/or evaluation.

2.3.2 FSA will only use client information for those purposes for which it was acquired, or with the written consent of the client for a related purpose, or where required by law.

2.3.3 FSA will not disclose any personal client information to third parties, including whether someone is known to the organisation's counselling services, except where disclosure is explicitly allowed for by this policy.

2.3.4 Where this policy allows for the disclosure of client information, staff will disclose only that information which is necessary to achieve the relevant purpose.

2.4 Collection of personal and sensitive client information

2.4.1 FSA may collect and record personal, sensitive and health information directly from clients including a client's name, address, ethnicity, date of birth, trauma history, clinical history, presenting

issue, referral details, information about the content of counselling sessions, assessment details and interventions provided.

2.4.2 Where the client is accessing a service with a specific requirement FSA may also collect relevant additional information.

2.4.3 FSA will not record a client's telephone number except where:

- the client provides verbal consent to do so; or
- the counsellor identifies a duty of care because the client or another person is at risk of harm; or
- FSA is required by law to do so.

2.4.4 FSA will never voice record counselling phone calls.

2.4.5 FSA will record the transcript of online counselling contacts.

2.5 Client right to remain anonymous

2.5.1 Clients have a right to remain anonymous when engaging with any FSA counselling service.

2.5.2 However, where a client chooses to remain anonymous, this may affect the quality of counselling services provided and/or the client's ability to access or correct their personal information.

2.6 Disclosure of identifying client information to other FSA staff

2.6.1 FSA upholds client confidentiality within the counselling team rather than by one counsellor. The counselling team includes counsellors, supervisors and the Director of Counselling Services. The counselling team may share information through written communication and verbally, during handover, team meetings and supervision. The purpose of sharing information in this context is to improve the quality of service provision.

2.6.2 Where necessary, the Chief Executive Officer, the Legal Projects Worker and administrative staff may also access sensitive client information.

2.7 Disclosure of identifying client information to third parties

Identifying client information will only be disclosed to a third party where:

2.7.1 FSA identifies a duty of care to the client or another person who is at risk of harm.

2.7.2 A client provides written and fully informed consent for FSA to release information to Police.

2.7.3 A client provides written and fully informed consent to FSA to release information to the **client's solicitor or other service provider**, including reports for Victims Services.

2.7.4 A client provides written and fully informed consent for FSA to consult with **third party service providers** in relation to therapeutic planning and clinical care networking.

2.7.5 A client provides fully informed, verbal consent for FSA to disclose information to a third party as part of a referral process.

2.7.6 FSA have a **legal obligation** to disclose information to a third party, for example under a subpoena. FSA will always seek to inform and consult with a client about the receipt and content of a subpoena. Where FSA determine that compliance with the subpoena may not be in the client's interests, FSA will seek to claim communications privilege.

2.7.7 A client has died and a subpoena for client information is received from the **Coroner's Court**.

2.7.8 A client discloses to FSA that they have perpetrated sexual, family or domestic violence or another serious crime.

2.8 Disclosure of non-identifying client information to third parties

2.8.1 FSA may disclose non-identifying client information where:

- A staff member discusses their work with an External Counselling Professional for the purpose of mitigating the risks of vicarious trauma.
- Reports containing non-identifying statistical information are provided to the Board, funding bodies, stakeholders, and other interested individuals and bodies.

2.8.2 Non-identifying information must not include any details that may identify a client or lead a client to feel they have been identified. For example, FSA will not disclose statistical information where the parameters of the report are so narrow that a client may feel they have been identified.

3 Staff Information

3.1 Collection of personal and sensitive staff information

3.1.1 FSA may collect personal and sensitive information about staff members including their full name, home address, private telephone number, bank details, next of kin, superannuation details, tax numbers, and shift times.

3.1.2 FSA will not conduct surveillance of any staff members or record phone calls between counsellors and clients. However, with client consent, call monitoring by a Supervisor may occur for the purpose of performance, training and quality improvement.

3.1.3 In rare circumstances, a staff member's access to the client management system may be monitored for the purpose of responding to a complaint or concern raised about that staff member's conduct.

3.2 Purpose and use of collecting staff information

3.2.1 Staff information will only be used for work related purposes, including to make contact with staff members and to make salary payments.

3.2.2 FSA will not disclose any sensitive information about staff members to clients or any other individual or group. This policy exists to protect staff members' safety and to promote healthy boundaries between professionals and clients.

3.2.3 Where necessary, staff members may provide the personal information of the Chief Executive Officer to third parties.

3.3 Breaches of staff confidentiality

3.3.1 Where any staff member considers that a breach of confidentiality may have occurred, they are to immediately notify a Counselling Services Manager or other person in an equal or more senior position. The person notified will verify the circumstances and if a breach has or may have occurred inform the Director of Counselling Services or the Chief Executive Officer, whoever is more immediately available. This person will investigate the breach and treat it as a critical incident according to 2.8 Critical Incident Management.

3.3.2 Where a staff member's confidentiality has been breached, FSA will notify the staff member unless there are compelling professional, ethical or legal reasons not to. Where a staff member is not notified, this decision and the reasons for the decision must be recorded and stored on their personnel file.

4 Supporter and Donor Information

4.1 Collection of personal and sensitive supporter and donor information

4.1.1 FSA may collect personal and sensitive information about supporters and donors including their name, contact details and credit card or other payment details.

4.1.2 FSA may collect information directly from supporters or donors when they provide this information to the organisation in person, in writing, via email, via the telephone, or via our website.

4.1.3 FSA may also collect information from third parties including those who collect donations on behalf of FSA.

4.2 Opting out of receiving information from FSA

4.3.1 Any person/organisation can opt out of receiving communications from the FSA at any time.

4.3.2 This can occur through the use of the clear links provided in all digital communication or by contacting FSA by telephone or email.

4.3 Purpose and use of collecting supporter and donor information

4.3.1 FSA collects supporter and donor information for the purposes of communicating with supporters and donors about goods, services, programs relevant to the work of the organisation, and for processing donations.

4.3.2 FSA may disclose supporter and donor information to third parties where:

- Disclosure is required by law;
- Where a donor or supporter provides informed consent for FSA to acknowledge their contribution publicly.

4.4 Disclosure of personal information to overseas recipients

4.4.1 FSA may store donor and supporter information using a third-party cloud-based storage system. This means that personal information in relation to donors and supporters may reside on servers based in Australia and/or the USA.

4.4.2 FSA takes reasonable steps to ensure that any overseas recipient does not breach the Australian Privacy Principles in relation to the information.

5 Website

5.1 FSA collects statistical information about the computer hardware and software of users of our site using Google Analytics. This information can include browser type, country, and access times. No personally identifying information about any user is recorded or provided to Google. As with all websites, visitor IP addresses are stored in our server log files. These will never be linked to any personal information unless required by law.

5.2 As with all websites, the FSA website uses cookies to collect personal information. Cookies are small text files that the website transfers to your computer through your web browser to enable the website's systems to recognise your computer. We use cookies to measure how often people visit our site and how they use it. We use this information to make improvements so that users have a better experience.

5.3 Our website contains hypertext links to other third-party websites. We are not responsible for the privacy practices or the content of such websites, which are governed by third party privacy policies.

6 Storage and Security

6.1 **Security** safeguards

6.1.1 FSA will implement reasonable security safeguards to protect against unauthorised use, disclosure, loss or other misuse of personal information.

6.1.2 All persons who may have access to personal client or staff information will be required to sign an agreement which obliges them to comply with the Privacy and Confidentiality Policy.

6.1.3 Access to electronically-stored client information will be restricted through security measures including password protection, firewalls, and data encryption for any information transfers and storage. Hard or paper copies of client information will not be kept.

6.1.4 Access to work areas where client information is stored will be restricted through pass code access. Where a visitor is required to access or view areas that client information is stored, staff will take all reasonable precautions to maintain privacy and confidentiality.

6.2 Retention of client files

6.2.1 Client files created after 2006 will be retained for at least the retention period designated below. The retention period will be

measured from the client's last contact with the service or contact by another with the service on behalf of the client, or 7 years after the client turns 18 years, after the completion of any related legal action which the service is aware of, or after the last contact for legal access purposes, whichever is later.

Type of record	Designated retention period
All client files	7 years
Client files which contain an allegation of sexual assault	30 years
Client files which contain an allegation of child sexual abuse	45 years
Client files which contain an allegation of physical abuse and/or neglect	30 years
Any record relating to the handling of complaints and the investigation of incidents concerning client care	7 years
Any subpoena or disclosure order and related correspondence	7 years

6.2.2 Where a client file was created prior to 2006, the client file may have been destroyed 7 years after the client's last contact with the service or contact with the service on behalf of the client, or 7 years after the client attained the age of 18 years, whichever was later.

6.3 Deletion of Client Files

6.3.1 FSA will not delete any client file prior to the mandatory legal retention period. In most cases, this will be 7 years after the client's last contact with the service or contact with the service on behalf of the client, or for 7 years after the client attains the age of 18 years, whichever is longer.

6.3.2 Where a client requests that their file be deleted after the conclusion of the mandatory legal retention period, FSA will endeavor to fulfill the client's request unless there are compelling professional, ethical or legal reasons not to.

6.3.3 Where a client file is to be deleted FSA will keep a record of the name of the individual to whom the information related, the period covered by it and the date on which it was deleted or disposed of.

7 Right to Access and Correct Personal Information

7.1.1 Clients, supporters and donors have a right to access and correct any personal information that FSA holds about them.

7.1.2 All requests for access or correction should be made to the organisation in writing using the contact details in Section 10.

7.1.3 FSA will take reasonable steps to confirm an applicant's identity before granting access to or correcting personal information.

7.1.4 FSA will not refuse any reasonable request to access or correct personal information, unless there are compelling professional, ethical or legal reasons for refusing access and an exception in Australian Privacy Principle 12.3 applies.

7.1.5 FSA will acknowledge receipt of all requests for access or correction within 5 working days after receiving the request.

7.1.6 FSA will seek to provide an outcome to all requests for access or correction as soon as possible, and always within 45 days after receiving the request.

7.1.7 Where a request for access or correction is denied, FSA will provide the applicant with written reasons for that denial.

8 Complaints

8.1.1 Where a person believes that FSA may have breached their privacy or confidentiality, they should contact the organisation using the contact details in Section 10.

8.1.2 The full complaint process is outlined in 2.7 Complaints and Compliments Policy.

9 Data Breaches

9.1.1 All data breaches will be managed in compliance with the Notifiable Data Breaches Scheme according to the following procedures: 2.5a Data breach response plan and 2.8 Critical Incident Management.

10 Contact Details

10.1.1 If you have any queries relating to this Privacy and Confidentiality Policy, please contact our Staff on:

Phone: (02) 8585 0333

Fax: (02) 9555 5911

Postal Address: PO Box 555, Drummoyne NSW 2047

Email: info@fullstop.org.au