

FSN Privacy Policy

Date this policy was adopted by the Management Committee: 7/08/2014

Table of contents:

Purpose	2
Definitions.....	2
Policy	2
The use of government identifiers.....	2
Responsibilities	3
The purposes for which FSN collects, holds, uses and discloses personal information, and the consequences of not providing such information.....	3
Clients have the right in regards to child protection notifications to.....	3
Use and disclosure of personal information.....	4
Related documents	4
Procedures	4
How an individual may gain access to and seek correction of information:.....	4
The Freedom of Information Act 1982 (FOI Act) gives any person the right to:	5
Refusal to give access.....	5
How to make an FOI request.....	6
How an individual may complain to you about a breach of the APPs and how such a complaint will be dealt with by you.....	6
Other entities that FSN usually discloses information to.....	6
Direct Marketing by FSN.....	6
Data quality and security.....	6
Job applicants.....	7
Staff.....	7
Updates to this Policy.....	7
References	8

Purpose

From **March 12**, 2014, the Australian Privacy Principles (APPs) replaced the National Privacy Principles (NPPs). FSN is bound by the NPPs contained in the Privacy Act 1988 (Privacy Act) and has updated its Privacy Policy in light of these changes. FSN is committed to protecting confidential and private information of individuals of all ages.

The APPs deal with the collection, use and disclosure, quality, security, access to and correction of personal and sensitive information. Family Support Network’s APP will be available on our web site www.fsn.org.au If a person or body requests a copy of FSN’s APP in a particular form, FSN will take such steps as are reasonable in the circumstances to give the person or body a copy in that form.

From time to time FSN may make changes to our policy, processes and systems in relation to how we handle your personal information. We will update this Privacy Policy to reflect any changes. Those changes will be available on our website and at our head office.

Definitionsⁱ

“**Personal information**” now means *information or an opinion* about an identified individual, or an individual who is reasonably identifiable, whether or not the information or opinion is true and whether or not it is recorded in a material form.ⁱⁱ

“**Sensitive information**” includes an information or opinion about an individual’s *racial or ethnic origin, political opinions, membership of a political association or professional or trade association or trade union, religious beliefs or affiliations, philosophical beliefs, sexual orientation or practices, criminal record, health information, genetic information*, and now also includes: biometric information (examples of biometric info are information about a specific person's body, hair colour, height, their *fingerprint or DNA sequence*ⁱⁱⁱ that are used for automated biometric verification or biometric identification)

Policy:

This policy relates to the kinds of personal information that FSN will collect and hold, and how FSN collects and holds such personal information:^{iv}

FSN will only consensually collect information that it believes to be necessary and relevant to help us safely provide services to clients. This includes the client’s name, address, contact details and date of birth. FSN will also ask for the names and dates of birth of your family. FSN will also ask clients to inform us of what sort of issues are affecting them and what sort of support they would like to help their family achieve their goals. We collect information in various ways, such as over the phone, from a referral via fax or in writing, in person, or over the Internet. Clients should take appropriate security precautions when using the Internet to communicate with FSN. Clients should also take reasonable steps to protect their personal and sensitive information when using social media such as Facebook. Clients can be referred to FSN by another service provider (with the client’s permission where practical) or they can refer themselves to FSN.

We may also ask clients if they or their family identify as ATSI to help with our reporting to our funding bodies, if they speak a language other than English at home. **Reporting to funding bodies by FSN is always anonymous from a client perspective**, therefore clients can not be identified.

This information may initially be recorded on a paper file and then transferred to an electronic database. Client information is stored in a safe, secure way, including a password protected computer system. FSN will take reasonable steps to ensure that the personal information is protected from misuse, loss, unauthorised access, modification or disclosure, and interference. This will involve passwords being changed regularly. FSN will take reasonable steps to ensure that client information is accurate, up-to-date and complete. FSN will take reasonable steps to destroy or de-identify personal information which is no longer needed for the purposes for which it may have been intended or disclosed where it is lawful and reasonable to do so^v. However this requirement will always be subject to any laws or requirements by our funding bodies concerning the need to retain client information. Currently our funding bodies require us to keep client information for a minimum of 7 years. FSN will also provide the source of the individual’s personal information, if asked by the client unless it is impracticable or unreasonable to do so.^{vi}

The use of government identifiers^{vii}

FSN will not adopt, use or disclose a government related identifier (such as Medicare numbers or Driver licence numbers, Passport numbers and Centrelink reference numbers) unless:

- the adoption, use or disclosure is required or authorised by law
- it is reasonably necessary to verify the identity of the individual

- it is reasonably necessary to fulfil obligations to a Commonwealth agency or state or territory authority or to help a client deal with these organisations
- FSN reasonably believes it is necessary to lessen or prevent a serious threat to the life, health and safety of an individual or to public health and safety
- FSN reasonably believes that use or disclosure is necessary for the practice to take action in relation to suspected unlawful activity or misconduct of a serious nature
- FSN reasonably believes that the use or disclosure is reasonably necessary for enforcement related activities of an enforcement body.

Responsibilities:

The purposes for which FSN collects, holds, uses and discloses personal information, and the consequences of not providing such information.

To help provide the best support for families, ensure the safety of staff, and ensure FSN is meeting its funding requirements, FSN collects the above client information. If a client is referred to FSN by another service, FSN may provide feedback to the referrer on whether the referral was appropriate and helpful to the client. This information is held until the client ceases to receive services from FSN. FSN is currently required by its funding bodies to then hold client information for a minimum of 7 years after the client has ceased receiving services from FSN. After 7 years FSN will destroy any hard copies of client information. If a client would benefit from receiving services from other service providers FSN would discuss this with the client and if the client wishes, FSN will provide relevant client information to the other service provider.

FSN also has a legal responsibility to advocate on behalf of children who are at risk of harm to the relevant authorities. Harm includes violence or abusive behaviour of any kind. For example physical abuse (including physical discipline that is seen to harm the child), emotional abuse or torment, neglect of physical needs, sexual abuse, and / or any other behaviours that threaten a child's right to safety. FSN would notify the relevant authorities (including the Police and Family and Community Services) if:

- we were told (by a child or parent / adult) that a child's safety was at risk or that they were being harmed in some way or,
- if we hold concerns from our own observations about a child's safety.

Clients have the right in regards to child protection notifications to:

- Be clearly told about your responsibilities in relation to child protection and safety and of what actions the service will take if a child is at risk and / or is being harmed. (Before any ongoing support work is commenced).
- Ask more specific questions about the notification process and / or our own guidelines at any time.
- Be told that a notification is to be made and why (we reserve the right to not give you prior notice if there is a concern that this will further endanger the child and / or another person and / or the worker).
- Make the notification yourself, with our support, if you so desire.
- Continue to be supported after a notification is made.
- Be referred to a different agency if you no longer want to work with this service after a notification has been made.
- Make a suggestion, comment or complaint about our services in a timely and fair manner.

Use and disclosure of personal information^{viii}

FSN will only use or disclose personal information for a "primary purpose" or a "secondary purpose." A "primary purpose" is the particular purpose for which the information was

collected. The Information Commissioner's Guidelines state that this purpose should be narrowly construed so clients understand how their information will be used.

A "secondary purpose" can arise in these circumstances:

- Consent – a client consents to the secondary use. This consent can be express or implied, but the patient must have capacity to give consent. The consent must also be informed and current.
- Reasonable expectation of clients that information will be used or disclosed for a different purpose closely related to the primary purpose. The "secondary purpose" is directly or closely related to the "primary purpose".
- Disclosure is required or authorised by law. For example:
 - Warrant from Police to access client records
 - Subpoena to produce documents or give evidence
 - Mandatory notification of child abuse or notifiable diseases
- There is a "*permitted general situation*" – situations when personal information can be disclosed for a "secondary purpose" (section 16A) including:
 - Health and Safety – if FSN has a reasonable belief that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of an individual or to public health or safety, and it is unreasonable or impracticable to obtain consent from client. There is no longer a requirement that the threat is "imminent", but it must still be serious.
 - Unlawful activity / serious misconduct – if FSN has a good reason to suspect that unlawful activity or misconduct of a serious nature that relates to the practice's functions has been, or is being or may be engaged in and the use or disclosure of information is necessary for FSN to be able to take appropriate action.
 - Defending or establishing a legal or equitable claim – this is a new provision that confirms the right organisations to disclose information to respond to complaints or claims.
 - Confidential mediation / dispute resolution processes – this is another new provision that confirms the right of an organisation to use or disclose personal information during a confidential alternative dispute process such as a mediation.

Related Documents (where applicable):

Archiving and Document Destruction Procedure, Code of Conduct Policy and the Family Worker Procedures.

Procedures:

How an individual may gain access to and seek correction of information:

If clients feel we have inaccurate information about them on our records, they should talk to the FSN staff person they have been dealing with. If the matter isn't controversial, such as updating their contact details, clients could also contact the FSN's Admin staff. If clients wish to gain access to their information, they would need to make a written Freedom of Information (FOI) application and either email, post or fax the request to the FSN General Manager (GM@fsn.org.au), PO Box 236, Lismore NSW 2480, fax 02 6621 5208. A FOI request may take up to 30 days to process. Access for a client file may be given through the use of a mutually agreed intermediary. There is no fee for requesting information under the FOI act but there may be a charge that is not excessive for supplying the information. See www.fsn.org.au for a copy of our form for obtaining information under FOI.

The Freedom of Information Act 1982 (FOI Act) gives any person the right to: ^{ix}

- access copies of documents we hold (some exemptions may apply – see below for more details)
- ask for information we hold about you to be changed or noted if it is incomplete, out of date, incorrect or misleading, and you can ask to see your file, **however we can refuse access to some documents, or parts of documents if:**
 - (a) FSN reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or
 - (b) Giving access would have an unreasonable impact on the privacy of other individuals; or
 - (c) The request for access is frivolous or vexatious; or
 - (d) The information relates to existing or anticipated legal proceedings between the FSN and the client, and would not be accessible by the process of discovery in those proceedings;
 - (e) Giving access would reveal the intentions of FSN in relation to negotiations with the client in such a way as to prejudice those negotiations; or
 - (f) Giving access would be unlawful;
 - (g) Denying access is required or authorised by or under an Australian law or a court / tribunal order; or
 - (h) Both of the following apply:
 - (i) FSN has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to FSN's functions or activities has been, is being or may be engaged in;
 - (ii) Giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or
 - (i) Giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or
 - (j) Giving access would reveal evaluative information generated within the entity in connection with a commercially sensitive decision-making process or other matters set out in the FOI Act.

Refusal to give access^{xi}

If FSN refuses to give access to the personal information because of any of the above reasons or to give access in the manner requested by the individual, FSN will give the individual a written notice that sets out:

- (a) The reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so; and
- (b) The mechanisms available to complain about the refusal; and
- (c) Any other matter prescribed by the regulations.

How to make an FOI request:

You can submit your request by post, fax or email but your request must:

- be in writing
- state that the request is an application for the purposes of the FOI Act
- provide information about the documents to assist us to process your request
- provide an contact details for reply

If you ask a third party to make an FOI request on your behalf, you need to provide a specific, written authority to send copies of documents to you care of that person, or to allow that person to inspect copies of documents containing information about you. A copy of FSN's Freedom Of Information Application Form will be available on our web site and at our main office.

How an individual may complain to you about a breach of the APPs and how such a complaint will be dealt with by you:

If you feel FSN has breached the APP, you should talk to the FSN staff member you have been dealing with. If you are unhappy with their response, you can ask to speak to their manager. If you are unhappy with their response you can ask to speak to the General Manager. Any breach of the APP by a FSN staff member is considered a serious matter and will be dealt with accordingly.

Other entities that FSN usually discloses information to:

Client information can be disclosed to another service provider (with the client's permission) to help them obtain more services. If FSN has concerns about children being harmed we would notify the Police and Family and Community Services on the Child Protection Helpline (ph 132 111) and inform you in writing. Client's information may be passed on to relevant authorities if we believe that the client or another person may be at risk.

FSN does not provide client information to marketing companies or overseas companies.

Direct Marketing by FSN

FSN will not use or disclose sensitive information for the purpose of direct marketing unless the individual consents to the use or disclosure for that purpose. Direct marketing involves the use of personal information to communicate with an individual to promote goods and services. FSN may send out written promotional material directly to clients or organisations that would reasonably expect their personal information to be used for direct marketing. Anyone who receives direct marketing material from FSN will be made aware of how to opt out and FSN will comply with a request to opt out.^{xii} If you have subscribed to any of our newsletters or subscriptions and no longer wish to receive such communications, please call 6621 2489 or email us at Admin@fsn.org.au

Data quality and security

FSN will take reasonable steps to ensure that the personal information we collect is accurate, up-to-date and complete, and relevant to the services we provide to clients and could be substantiated in a court of law if necessary. FSN will therefore regularly check with clients that their contact details are up-to-date and accurate.

FSN will not be responsible for the accuracy of information or data provided by any third party.

FSN will take reasonable steps to ensure that the personal information we hold is protected from misuse, loss, unauthorised access, modification, disclosure, and from interference. FSN will take reasonable steps to destroy or de-identify personal information which is no longer needed (N.B. FSN is currently required by funding bodies to keep client information for a minimum of 7 years before destroying it).

FSN will not be liable for content on third party websites that may link from our own websites.

Job applicants.

If you apply for a position with us, we may also collect information about your qualifications, experience, character, screening checks (including health, reference, background, directorship, financial probity, identity, eligibility to work, vocational suitability, drugs / alcohol and criminal record checks). We collect, use and disclose your personal information to

assess your application, conduct screening checks and consider and contact you regarding other positions. We may exchange your personal information with academic institutions, recruiters, screening check providers, health service providers, professional and trade associations, law enforcement agencies, referees and your current and previous employers. Without your personal information we may not be able to progress considering you for positions with us.

Staff.

This section applies to our current and former employees and contractors in addition to the recruitment section above. We may collect information relating to your current or former employment or engagement including information about your training, disciplining, resignation, termination, terms and conditions, emergency contact details, performance, conduct, use of our IT resources, payroll matters, union or professional / trade association membership, recreation, leave and taxation, banking or superannuation affairs. We are required or authorised to collect your personal information under various laws including the Fair Work Act, Superannuation Guarantee (Administration) Act and Taxation Administration Act. We collect, use and disclose your personal information for purposes relating to your employment or engagement with us including engagement, training, disciplining, payroll, superannuation, health and safety, administration, insurance (including WorkCover) and staff management purposes. We may exchange your personal information with your representatives (including unions) and our service providers including providers of payroll, banking, staff benefits, security and training services. Without your personal information we may not be able to effectively manage your employment or engagement.

Updates to this Policy.

Our Privacy Policy will be reviewed from time to time to take into account new laws and technology, changes to our operations and practices and the changing business environment. The current version is accessible at www.fsn.org.au

References:

ⁱ <http://www.mst.com.au/news/Australian-Privacy-Principles-Privacy-Readiness-Checklist>

ⁱⁱ <http://www.mst.com.au/news/Australian-Privacy-Principles> and <http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-17-australian-privacy-principles>

ⁱⁱⁱ http://www.biometricidentitycards.info/articles/biometric_identity_cards.html

^{iv} <http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-17-australian-privacy-principles>

^v <http://www.mst.com.au/news/Australian-Privacy-Principles>

^{vi} <http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-17-australian-privacy-principles>

^{vii} <http://www.avant.org.au/Resources/Public/20130211-avant-guide-to-privacy-reforms/>

^{viii} <http://www.avant.org.au/Resources/Public/20130211-avant-guide-to-privacy-reforms/>

^{ix} <http://www.humanservices.gov.au/corporate/freedom-of-information/>

^x <http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-17-australian-privacy-principles>

^{xi} <http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-17-australian-privacy-principles>

^{xii} <http://www.avant.org.au/Resources/Public/20130211-avant-guide-to-privacy-reforms/>