



Commitment to Privacy

Family Support Network Inc. (FSN) is committed to protecting the privacy and confidentiality of all personal and sensitive information we collect. We respect the privacy rights of our participants, staff, volunteers, Board members and external stakeholders, and ensure that personal and health information is handled securely, ethically and in line with our legal obligations.

We comply with privacy and related laws, including:

- *Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act)
- *Health Records and Information Privacy Act 2002* (NSW) (HRIP Act)
- *Privacy Act 1988* (Cth)
- Australian Privacy Principles (APPs)
- *Children and Young Persons (Care and Protection) Act 1998* (NSW)
- *Government Information (Public Access) Act 2009* (NSW) (GIPA Act)
- *State Records Act 1998* (NSW)
- *Crimes Act 1900* (NSW) – Computer Offences
- *Health Insurance Act 1973* (Cth)
- Notifiable Data Breaches Scheme (*Privacy Act 1988* (Cth))
- NSW Health Privacy Guidelines
- Department of Communities and Justice (DCJ) Privacy Policies and Guidelines

These laws guide how we collect, store, use and disclose personal and sensitive information, whether in physical or electronic records, or verbal discussions.

Our Privacy Commitments

At FSN, we are dedicated to:

- Meeting all legal and ethical obligations as a service provider and employer in protecting privacy and confidentiality.
- Providing participants, staff, and other stakeholders with clear information about their rights to privacy.
- Obtaining informed consent before collecting, storing, using or disclosing personal and sensitive information.
- Ensuring privacy during interviews, case discussions, or any interactions involving sensitive or personal matters.
- Maintaining transparency in our operations while safeguarding individuals' privacy and protecting the confidentiality of our organisation's affairs.
- Making our privacy policy publicly accessible and available in alternative formats upon request, where reasonable.

- We expect all Board members, staff, and volunteers to uphold the confidentiality of FSN's business, as well as the privacy of individuals, organisations, and government partners with whom we work.

How We Manage Personal and Sensitive Information

Family Support Network collects, stores and disposes of personal and sensitive information in ways that protect privacy and maintain confidentiality. Our secure electronic systems and storage practices safeguard data related to participants, internal records, and organisational operations.

We will:

- Collect and retain information only when it is relevant and necessary for our services or operations.
- Inform participants about how their information is stored, managed, and shared.
- Consider cultural, linguistic or religious sensitivities when handling information.
- Securely store records for the period required by law or funding agreements.
- Ensure correct and secure transfer or disposal of records.

How We Collect Information

Personal and sensitive information may be collected in person, over the phone, via email, through our website, or by other electronic or paper-based methods. Paper records are stored securely and, where appropriate, scanned into our electronic systems and securely destroyed.

We only collect and use information that is:

- Relevant to the services we deliver or for purposes consistent with why it was provided.
- Required by law.
- Collected with express or implied consent.

Types of Information We Collect

1. Engagement with FSN

Information may be collected at different points depending on how individuals interact with FSN.

Examples may include:

- Referrals and intake processes
- Participation in programs or services
- Attendance at community events
- General enquiries
- Engagement through our website or newsletter subscriptions
- Recruitment of staff or volunteers
- Receipt of donations, bequests or other forms of support

Information collected may include:

- Name, suburb, postcode, and contact details
- Age or age group
- Consent for photographs or publication
- Details of advice, referrals, or support provided

We collect this information to:

- Provide tailored services to individuals and families.
- Monitor engagement and improve service effectiveness.

2. Information We Collect for Program Participants

For individuals accessing our core services (e.g. Family Work, Start Together, Intensive Family Preservation, Playgroup, parenting programs), we may collect the following details:

- Full name or pseudonym
- Date of birth
- Gender
- Address and contact details
- Country of birth, cultural background, and language spoken at home
- Aboriginal and/or Torres Strait Islander identity
- Disability status and type of disability
- Household composition and indicators of homelessness
- Other details where relevant (e.g. interpreter needs, education level, employment status, income, NDIS eligibility)

Other program participant records may include:

- Consent details
- Medical conditions and safety alerts
- Information relating to child protection or court orders
- Information shared with or received from other services
- Case notes, assessments, and plans
- Referrals, reports or letters relevant to the services provided

For participants in our youth-specific activities where parents are not present, additional details may be collected, such as:

- Health information (e.g. allergies, medications, dietary needs)
- Parent or guardian contact details
- Consent forms for excursions, photography, or liability waivers
- Information about safety incidents or feedback from events

3. Information We Collect for Funders

Under our funding agreements, including with DCJ, FSN is required to collect and report specific data, often through systems like the Data Exchange or InfoShare. Information may include:

- Name (or pseudonym)
- Date of birth
- Gender
- Residential suburb, state, postcode
- Indigenous status
- Cultural and linguistic background
- Disability status
- Consent for follow-up or data use

Where possible, this data is reported in de-identified formats to protect individual privacy.

For Intensive Family Preservation services, DCJ collects data such as names, addresses, session dates, and casework details through the InfoShare portal.

Participants will be informed about data collection requirements and may be asked to provide separate consent for certain data-sharing activities.

4. Wesley Mission Emergency Relief

Family Support Network partners with Wesley Mission to provide emergency relief support for individuals and families at risk of financial hardship. We only share information with Wesley Mission with explicit signed consent from participants. Information shared may include:

- Personal details (e.g. name, date of birth, address, gender, contact details)
- Household composition and financial circumstances
- Supporting documents (e.g. identification, bank statements, income statements, bills, rental arrears)⁴
- Serial numbers and amounts of vouchers issued

Disclosure of Personal Information

We will not share personal or sensitive information with third parties unless:

- You have provided express consent.
- It is necessary to protect the safety, wellbeing or welfare of children and young people.
- We are legally required or permitted to do so.

Under Chapter 16A of the *Children and Young Persons (Care and Protection) Act 1998* (NSW), consent is not required where information is exchanged for the safety, welfare or wellbeing of children.

Information may be shared with prescribed bodies such as:

- NSW Department of Communities and Justice (DCJ)
- NSW Health
- Schools and education departments
- NSW Police
- Allied health professionals
- Other non-government organisations providing services to children and families

Accessing Your Personal Information

Individuals have the right to request access to the personal information FSN holds about them and to request corrections if information is inaccurate, out-of-date or incomplete.

The PPIP Act provides rights to access personal information under section 14. The HRIP Act provides rights to access health information under Clause 7 of Schedule 1.

Requests can be made verbally or in writing, though we encourage written requests to ensure clarity and proper record-keeping. Please use the contact us form on our website to contact us in writing.

Data Breaches

If there is a breach involving personal information, FSN will:

- Identify and contain the breach
- Engage relevant authorities if criminal activity is suspected
- Notify affected individuals where appropriate
- Assess the severity and potential harm of the breach
- Review and strengthen security measures to prevent future breaches
- Report significant breaches to the Office of the Australian Information Commissioner (OAIC) if required

Use of External Tools and Websites

Family Support Network uses third-party platforms to help manage some of our administration and online communication. These services include:

- Mailing list tools such as Mailchimp
- Social media platforms such as Facebook and Instagram
- Our website, hosted via WordPress

We do not store sensitive personal information (such as health or case details) on these platforms. Information shared on these services is limited to general communication and engagement, such as newsletters, updates, or public information about our services and events.

Each of these third-party platforms has its own privacy policy, which we encourage you to review for information about how your data may be collected and used when interacting with FSN online.

Complaints

If you believe your privacy rights or the Australian Privacy Principles have been breached by FSN, our staff, Board members, or volunteers, you have the right to make a complaint. Complaints will be managed seriously and promptly, in line with FSN's Complaints Policy.

Contact Us

For any questions, requests, or complaints regarding privacy, please use the contact us form on our website www.fsn.org.au

Family Support Network is committed to maintaining the highest standards of privacy and confidentiality. We value the trust placed in us by participants, families, staff, volunteers, and the broader community, and strive to protect personal information in everything we do.