Privacy Policy

Ph: 07 3826 1500
Email: yfs@yfs.org.au
Feedback line: 07 3826 1596
PO Box 727 Woodridge Qld 4114
www.yfs.org.au

STATEMENT

YFS respects the privacy of clients, staff, volunteers, students, board members, sponsors, donors and business partners and is committed to safeguarding the personal and sensitive information provided to us.

YFS manages personal information in accord with the *Privacy Act 1988 (Commonwealth), Australian Privacy Principles (APPs), Information Privacy Act 2009 (IP Act), Queensland Privacy Principles (QPPs), and the Right to Information Act 2009 (IT Act)*.

YFS holds contracts to deliver State and Commonwealth government programs. In providing such services, we comply with the relevant state or Commonwealth privacy principles and any additional obligations under the contract.

The YFS Privacy Statement is available on the YFS website and the principle of limits to privacy is explained in the *Client Information Pocket Guide (101304)* and *Welcome to YFS Poster (100494).*

PURPOSE

This privacy policy clearly outlines:

- How YFS handles personal and sensitive information
- Why YFS collects personal and sensitive information and the sort of personal information that YFS holds
- How YFS adheres to the Notifiable data breaches scheme.

SCOPE

This policy applies to clients, staff, volunteers, students, board members, online users, sponsors, donors and business partners. The Privacy Act and this Privacy Policy do not apply to acts or practices which directly relate to employee records of current and former employees.

Training is provided to all staff during induction and as an annual refresher

DEFINITIONS

Online users refers to anyone that accesses the YFS website www.yfs.org.au or social media sites. For example, Twitter and Facebook.

Personal information as defined by the *IP Act and RTI Act* is information or an opinion about an identified individual, or an individual who is reasonably identifiable from the information or option whether true or not, and whether recorded in a material form or not. Personal information collected by YFS includes name, date of birth, contact and address details, educational qualifications etc.

Sensitive information as defined by the *IP Act* 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

Health information is a part of an individual's personal and sensitive information and includes information or an opinion about a person's health or disability. Health information is only collected if directly related to, the activities and functions provided by YFS.

Data breach is when personal information held by an entity is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference. Examples of a data breach are when a device containing personal information of clients is lost or stolen, an entity's database containing personal information is hacked or an entity mistakenly provides personal information to the wrong person. Refer to Appendix 1 – Data Breach.

REFERENCES

- *Privacy Act 1988 (Commonwealth)*
- *Australian Privacy Principles (Privacy Amendment [Enhancing Privacy Protection]) Act 2012 (incorporated in Privacy Act 1988)*
- *Information Privacy Act 2009 (Qld)*
- *Queensland Privacy Principles (QPPs)*

- *Right to Information Act 2009*
- *Human Rights Act 2019*
- *The Office of Australian Information Commissioner (Cth) – Section B: Key Concepts*
- *The Office of the Information Commissions (Qld) – Key Privacy Concepts (Enforcement agencies and activities)*
- *Feedback, Complaints and Disputes Policy (101169)*
- *Authority to Share Information (100174)*
- *Client Information Pocket Guide (101304)*
- *Control of Records procedure (100312)*
- *Code of Conduct (101140)*
- *Staff Induction: An Overview (102614)*
- *Client and Staff Consent to Release Information work instruction (100423)*
- *YFS Ltd Overview of Legislation Provisions (102355)*
- *YFS Safeguarding Manual (103065)*
- *Safeguarding Policy (103006)*

OUR OBLIGATIONS IN RELATION TO PRIVACY

This Privacy policy sets out how we comply with our obligations under the *Privacy Act 1988* (Privacy Act) (Cth) and *Information Privacy Act 2009 (Qld)*. We are bound by both the Australian Privacy Principles (APPs) in the Privacy Act and the Queensland Privacy Principles (QPP's) in the Information Privacy Act, which govern how we collect, use, disclose store and protect personal information. These principles also ensure individuals can access and correct their personal information and require us to manage privacy in a transparent, secure and lawful manner.

YFS also acknowledges that under section 41 of the Information Privacy Act 2009 (Qld), QPP codes of practice may be developed and approved to guide the application of specific privacy principles. YFS will actively monitor for any approved QPP codes and ensure compliance with them as part of our ongoing commitment to privacy best practice.

Collection of personal information

YFS collects personal and sensitive information in accordance with the APP's and the QPP's. Individuals may request to access a YFS service anonymously or by using a pseudonym, and where lawful, we will take all reasonable steps to accommodate this request.

The type and amount of personal and sensitive information collected depends on the nature of the interaction with YFS and is limited to what is necessary for, or directly related to, our functions and services. All collection is conducted lawfully, fairly and with transparency.

How we collect information

YFS collects personal information only when it is necessary for, or directly related to, our functions and services, and always by lawful and fair means.

Where possible, we collect personal information directly from the individual. In cases where information is obtained from third parties, YFS takes reasonable steps to inform the individual of the collection and its purpose, unless an exemption applies under relevant legislation.

Under the *Child Protection Reform Amendment Act 2017* YFS Specialist Service Providers may collect personal information from third parties without consent, when required to assess child protection needs and better inform family support interventions.

YFS collects staff information through supervision records and formal HR documentation.

Use and disclosure of personal information

YFS uses and discloses of personal information primarily for the purposes for which it was collected. YFS will not use or disclose an individual's personal information for any other purpose or to any third party, unless one of the below applies:

- an individual provides consent to disclose their personal information for a secondary purpose
- we think it is reasonably necessary for enforcement-related activities carried out by, or on behalf of, an enforcement body
- a secondary purpose is required or authorised under an Australian law, or court or tribunal order.

YFS does not use or disclose personal information for direct marketing purposes. YFS may take photographs and videos at events for use on the YFS website, social media, media and other publications. Signs are posted at event entrances advising attendees that images will be taken; to opt out they see YFS staff at the event to be issued a wristband. Photographers are instructed not to take images of people with wristbands. If they are snapped, they will be cropped out wherever possible.

Disclosure of personal information to overseas recipients

YFS does not routinely disclose personal information outside Australia. Where overseas disclosure is necessary, we comply with the requirements of the Privacy Act 1988 (Cth) and section 33 of the Information Privacy Act 2009 (Qld), which governs the transfer of personal information outside Queensland.

Before any transfer of information outside of Australia occurs, YFS undertakes a Risk Assessment to determine whether the recipient country has privacy protections substantially similar to those under Australian and Queensland law. If equivalent protections are not in place, YFS ensures privacy is safeguarded through contractual arrangements that bind the overseas recipient to comply with privacy obligations.

YFS also obtains informed consent from the individual prior to any overseas transfer of personal information. Where required under contractual agreements with Queensland Government Departments, YFS will seek written approval from the department before disclosing personal information overseas.

Currently, YFS only shares de-identified client data related to Functional Family Therapy – Child Welfare with Functional Family Therapy LLC CSS (Client Service System) in the United States for quality assurance purposes. FFT LLC is subject to the privacy laws of its respective U.S. state. For further details refer to the: https://www.fftcss.com/Resources/FFT%20LLC%20Information%20Security%20Policy.pdf

Storage and security of personal information

YFS takes reasonable steps to protect the personal and sensitive information held, against unauthorised access, misuse, interference, loss, modification or disclosure.

Security measures include password-protected access to electronic systems (such as our client records), locked storage for physical records, and restricted access to authorised personnel only.

When personal information is no longer required for any lawful purpose, or is determined to be unsolicited and not needed, YFS securely disposes of the information in accordance with our *Control of Records procedure (100312)* and applicable legal obligations.

Access to and correction of personal information

YFS respects individuals' rights to access and correct their personal information, in accordance with the APP's and QPP's. Upon request, we will provide access to personal information we hold or make corrections, unless there is a lawful reason to refuse under the Information Privacy Act 2009 (Qld), the Privacy Information Act 1988 (Cth), the Right to Information Act 2009, or other applicable legislation.

Access to records is managed with in accordance with the *YFS Control of Records Procedure (100312)*. Access may be denied if the request:

- poses a serious threat to the life, health or safety of any person or to public health or safety
- unreasonably impacts the privacy of others
- is frivolous and vexatious
- relates to existing or anticipated legal proceedings
- would prejudice negotiations with the individual making the request
- is unlawful or is prohibited by law
- is not authorised or required by law
- prejudices law enforcement activities
- prejudices an action in relation to suspected unlawful activity, or misconduct of a serious nature relating to the functions or activities of YFS
- discloses YFS's commercially sensitive decision-making process or information
- meets any other exemption permitted under the APP's or QPP's.

If access is refused, YFS will provide written reasons. Disputes regarding access or correction will be managed in accordance with the *YFS Feedback, Complaints and Disputes policy (101169).*

1. **Staff responsibilities**

   YFS staff are informed of their legal and ethical obligations to protect privacy. This includes:

   - Induction and training upon commencement of employment
   - *Annual refresher training*
   - Signing of the *YFS Code of Conduct (101140)*
   - Regular supervision sessions.

2. **Privacy Contact Officer**

   The responsibilities of the Privacy Contact Officer are undertaken by the Property and Business Manager, in consultation with management and the CEO. The Privacy Contact Officer is responsible for:

   - Providing guidance on privacy-related matters
   - Assisting with privacy complaints and breach responses
   - Coordinating internal privacy training and awareness
   - Supporting managers in liaising with government departments regarding contractual privacy obligations.

3. **Informing direct service clients about privacy**

   Clients are informed about how their personal information is used and disclosed through the YFS *Client Information Pocket Guide (101304)* and other materials. These resources explain circumstances where privacy may be limited.

4. **Limits to privacy**

   Privacy may be limited in specific situations, including:

   - Risk of harm to self or others
   - Concerns relating to harm, neglect or risk of being harmed (including instances relating to child protection or a person with a disability)
   - Written requests for information release from clients or staff
   - Court/Tribunal orders for YFS to make records available
   - External party investigations of a serious complaint or incident and to check the quality of work (e.g. funding bodies, Work Cover, etc.)
   - Formal staff supervision processes.

   Decisions to release personal information are made in consultation with Client Service Managers. Subpoena requests are managed under the Subpoena Work Instructions (101398).

5. **Sight and sound privacy**

   YFS staff are responsible for maintaining confidentiality through:

   - Conducting client and staff meetings in spaces that provide for privacy and confidentiality
   - Discussing client matters discreetly and only on a need-to-know basis
   - Avoiding client discussions in public or communal areas (including during breaks and outside of work time)
   - Following the clear desk policy: securing files immediately after use and avoiding unattended paperwork. This includes paperwork and files relating to clients and staff. Physical documents and files must be kept in locked filing cabinets and returned to the cabinet immediately after use. No documents or files are to be left unattended on desks, at printers, nor stored in staff member's diaries or in-trays.

YFS Website and Social Media

YFS does not attempt to identify individuals who browse our website or engage with our social media platforms. In accordance with our obligations under the Privacy Act 1988 (Cth) and the Information Privacy Act 2009 (Qld), we do not collect personal information unless it is necessary for our functions and activities.

Where our website or social media pages contain links to third-party sites—whether government or non-government—YFS is not responsible for the privacy, security, or content of those external sites. Any activity on those sites is governed by their respective privacy policies.

Donors and Supporters

YFS collects personal information from donors and supporters only when it is necessary to carry out our functions and activities. In general, YFS only ever records information that has been provided directly by the individual.

The information collected is used to:

- Process donations
- Issue receipts and acknowledgements
- Respond to enquiries or feedback
- Provide requested information about YFS
- Seek support for continuing our work
- Improve our services through feedback

Donors and supporters can at any time choose not to receive any further communications from YFS or to alter the frequency and type of communications received. Please contact us to arrange this or if you would like further information.

Disclosure

YFS does not sell, rent, or otherwise provide personal information about donors or supporters to third parties for unrelated purposes.

We will only disclose personal information with the individual's consent, or where required or authorised by law, or in accordance with any exemption under the APP's or QPP's.

Personal information will only be published in YFS communications or promotional materials with the express permission of the individual.

Changes to this Privacy Policy

YFS reviews this Privacy Policy annually and updates it as required to reflect changes in legislation, including the Privacy Act 1988 (Cth) and the Information Privacy Act 2009 (Qld), or to improve our privacy practices.

Complaints

If you have a complaint about how YFS handles your personal information or believe we have breached our obligations under the Privacy Act 1988 (Cth) or the Information Privacy Act 2009 (Qld), you can contact us via:

- **Email:** yfs@yfs.org.au
- **Website:** http://www.yfs.org.au
- **Feedback line:** (07) 3826 1596
- **Mail:**
  CEO
  YFS Ltd.
  PO Box 727
  Woodridge QLD 4114

All complaints are managed in accordance with the YFS Feedback, Complaints and Disputes Policy (101169). We aim to respond to privacy complaints within 45 days.

If you are not satisfied with our response, or if you do not receive a response within 45 days, you may escalate your complaint to:

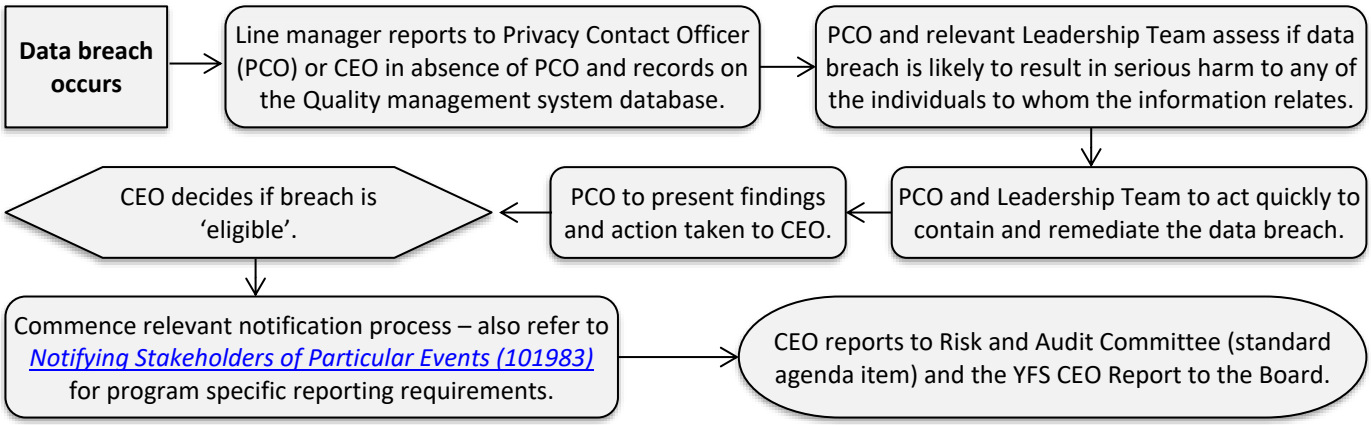
- The Office of the Australian Information Commissioner (OAIC) for matters under Commonwealth law: http://www.oaic.gov.au
- The Office of the Information Commissioner Queensland (OIC) for matters under Queensland law: http://www.oic.qld.gov.au

If the matter remains unresolved, you may request that the OIC refer the complaint to the Queensland Civil and Administrative Tribunal (QCAT) for formal review and decision.

APPENDIX 1 - ELIGIBLE DATA BREACH – *(SEE DEFINITIONS)*

YFS uses resources provided by the Office of the Australian Information Commissioner to assist in our planning and processes for Notifiable Data Breaches under the Privacy Act 1988 (Cth).

https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme



YFS is required to notify the OAIC and affected individuals when a data breach involving personal information is likely to result in serious harm. If an 'eligible' data breach' occurs YFS will:

1. Submit a formal statement to the OAIC in the required format.
2. Notify affected individuals directly, where practicable.
3. Where direct notification is not practicable, publish a copy of the statement to the YFS website and take reasonable steps to publicise its contents.
4. Notify our insurer, funding bodies and other critical stakeholders in accordance with internal procedures (refer to *Notifying Stakeholders of Particular Events (101983)*).

Risk Evaluation

YFS will assess the breach to determine:

a. The type and sensitivity of personal information involved
b. The context and cause of the breach
c. The extent of exposure or unauthorised access due to the breach
d. The likelihood of serious harm to affected individuals
e. The potential of other harms (e.g. reputational, financial).

Notification Considerations

Notification will be made to mitigate or prevent serious harm. Factors include:

- Whether individuals can take steps to reduce harm (e.g. change passwords, monitor accounts)
- Whether the compromised information is sensitive or likely to cause distress
- Legal and contractual obligations to notify, and the consequences of notification.

Queensland Specific Obligations:

Where personal information is handled under a Queensland Government contract, YFS will:

- Notify the relevant department of any privacy breach as soon as practicable, in line with contractual obligations
- Comply with section 33 of the Information Privacy Act 2009 (Qld) regarding overseas disclosure
- Monitor and comply with any future QPP codes approved under section 41 of the IP Act.

Legal and Contractual Risk Assessment:

As part of the breach response, YFS will:

- Assess whether the breach involves sensitive information or overseas disclosure
- Determine if obligations under any approved QPP codes are triggered
- Seek legal advice where appropriate
- Review and update internal privacy and security measures.

The relevant department may oversee YFS's breach response from a contract management perspective but does not provide legal advice. YFS remains fully responsible for containment, notification, remediation, and compliance with all privacy obligations.