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)* and *Australia Privacy Principles (Privacy Amendment [Enhancing Privacy Protection]) Act 2012*.

YFS holds contracts to deliver State and Commonwealth government programs. In providing such services, we comply with the relevant state or national 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 will clearly outline:

- How YFS handles personal and sensitive information
- Why YFS collects personal and sensitive information and the sort of personal information that YFS holds.

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.

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 *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. Personal information collected by YFS includes name, date of birth, contact and address details, educational qualifications etc.

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

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.

REFERENCES

- *Privacy Act 1988 (Commonwealth)*
- *Australian Privacy Principles (Privacy Amendment [Enhancing Privacy Protection]) Act 2012 (incorporated in Privacy Act 1988)*
- *Complaints and Disputes Policy (101169)*

- *Authority to Gain or Release Information and Appointment of an Advocate form (100174)*
- *Client Information Pocket Guide (101304)*
- *Control of Records procedure (100312)*
- *Social Media work instructions (101395)*
- *Code of Conduct (101140)*
- *Induction Guide (101828)*
- *Client and Staff Consent to Release Information work instruction (100423)*

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 information

If you would like to access a YFS service 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.

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

How we collect information

YFS will only collect personal information necessary for, or directly related to, its activities and functions and only by lawful and fair means. YFS' preference is to collect personal information directly from the individual. On occasion we may obtain personal information from a third party source. In such instances, YFS will take reasonable steps to contact the individual to ensure you are aware of the purpose for which we are collecting your personal information. YFS collects staff information through supervision records and formal HR documentation.

Use and disclosure of personal information

Other than the primary purpose for which information is being collected, we may also disclose your personal information to other external organisations including:

- government departments/agencies who provide funding for YFS services
- contractors who manage some of the services we offer to you. For example, contractors attending YFS managed properties for maintenance requests. 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 perform the functions required by YFS
- doctors and health care professionals, who assist us to deliver our services
- other regulatory bodies, such as WorkSafe
- referees and former employers of YFS employees and volunteers, and candidates for YFS employee and volunteer positions
- our professional advisors, including our accountants, auditors and lawyers.

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

- you have given consent
- you 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.

We do 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.

YFS does not use or disclose personal information for direct marketing purposes.

YFS take photographs and videos at events for use on the YFS website, social media, media and other publications.

YFS post signs at event entrances advising attendees that images will be taken; to opt out they see staff at the YFS stall 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.

Storage and security of personal information

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

These steps include password protection for accessing our client records SRS, 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, or is determined to be unsolicited personal information, it is disposed of in a secure manner, or deleted according to our *Control of Records procedure (100312).*

Eligible data breach

YFS are required to provide notice when data security incidents compromise an individuals' personal information and they are likely to suffer serious harm as a result.

If an 'eligible' data breach' occurs YFS will:

1. give a statement to the Information Commissioner in the appropriate form;
2. where practicable, notify the individual or individuals who are impacted by the data breach;
3. where individual notification Is not practicable, publish a copy of the statement to the YFS website and take reasonable steps to publicise the contents of the statement; and
4. notify our insurer.

YFS will evaluate the risks associated with the breach with consideration to the following factors:

a. the type of personal information involved
b. the context of the affected information and the breach
c. the cause and extent of the breach
d. the risk of serious harm to the affected individual/s

e. the risk of other harms.

Notification will occur to avoid or mitigate serious harm to an affected individual. The following factors will be considered when decided whether notification is required:

- What is the risk of serious harm to the individual as determined by the risk evaluation?
- What is the ability of the individual to avoid or mitigate possible harm if notified of a breach (in addition to steps taken by YFS)? For example, would an individual be able to have a new bank account number issued to avoid potential financial harm resulting from a breach? Would steps such as monitoring bank statements or exercising greater vigilance over their credit reporting records assist in mitigating risks of financial or credit fraud?
- Even if the individual would not be able to take steps to fix the situation, is the information that has been compromised sensitive, or likely to cause humiliation or embarrassment for the individual?
- What are the legal and contractual obligations to notify, and what are the consequences of notification?

Once the immediate steps are taken to mitigate the risks associated with the breach, YFS will investigate the cause, review the existing privacy policy and update our security measures as necessary.

YFS use the resources provided by the Office of the Australian Information Commissioner to assist in our planning and processes for Notifiable Data Breaches. https://www.oaic.gov.au/engage-with-us/consultations/notifiable-data-breaches/

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.

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

- YFS believes 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 between YFS and the individual
- providing access would prejudice negotiations with the individual making the request
- access would be unlawful
- denying 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 YFS
- access discloses YFS's commercially sensitive decision making process or information
- any other reason that is provided for in the APP's 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 *YFS Complaints and Disputes policy (101169).*

1. Staff responsibilities

YFS staff are informed about the legal and ethical responsibilities to protect client and staff privacy. Legal requirements and YFS privacy procedures are covered in:

- induction meetings
- *Induction Guide (101828)*
- signing of the *YFS Code of Conduct (101140)*
- supervision meetings

2. Informing direct service client about their privacy

Through the YFS *Client Information Pocket Guide (101304)* and other one-off client handouts or posters, clients are informed of how information about them will be used within and outside the service, and the circumstances under which privacy may not be maintained.

3. Limits to privacy

The following circumstances provide exceptions to the privacy process:

- situations in which clients and/or staff pose a danger to themselves or others (suicide and violence)
- situations if there is harm and neglect or risk of being harmed (child protection or a person with a disability)
- situations in which clients and staff request that their information or records be released to others in writing
- situations in which a Court/Tribunal orders YFS to make records available
- situations when an external party is investigating a serious complaint or incident and checking the quality of work (e.g. funding bodies, Work Cover, etc.)
- situations of formal supervision of a worker

A court of law may request client information from YFS by applying a Subpoena - refer to *Subpoena Work Instructions (101398).*

The releasing of private information is not carried out in isolation by workers. Such decisions are made in consultation with Client Service Managers/General Manager – Client Services.

4. Sight and sound privacy

It is the responsibility of staff to ensure privacy protocols are maintained and a confidential environment is maintained by:

- ensuring contacts with clients and formal staff supervision sessions are conducted in spaces that provide for privacy and confidentiality
- ensuring any conversations that need to happen about a client related matter are done with the utmost discretion and on a need to know basis
- ensuring that staff do not discuss clients in public, during breaks and outside work time and communal areas (e.g. hallways, reception, cafes, restaurants, etc.)
- adhering to the clear desk policy: client, HR and supervision files are kept in locked filing cabinets, and returned to the cabinet immediately after use. No files/paperwork is to be left unattended on desks, nor stored in staff member's diaries or in-trays.

YFS Website and Social Media

No attempts are made to identify anyone browsing our website. Where our website and social media sites contain links to third party sites, both government and non-government, YFS is not responsible for the privacy or security practices or content of such websites. Your activity on those sites is covered by the privacy policies of those sites.

Donors and Supporters

YFS only collects information about donors and supporters that is necessary for us to properly conduct our services. In general, YFS only ever records information about you that you have provided to us.

The information we collect is used to:

- process donations
- thank you and issue receipts
- respond to your comments or questions
- provide information requested about YFS
- seek support for continuing our work
- feedback to continuously improve our services.

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

Disclosure

At no time will YFS sell, rent or give away any personal information about our donors or supporters for use by third parties.

We will only ever pass on donor or supporter personal information if we have their consent or we are required by law to do so.

We will only ever publish donor or supporter personal information in our communications or advertisements with the express permission of that person.

Changes to this Privacy Policy

This privacy policy will be reviewed annually or updated prior in accord with further privacy legislation changes.

Complaints

If you wish to read our Complaints policy, have a complaint about YFS privacy practices or our handling of your personal information, please contact us via email yfs@yfs.org.au, website www.yfs.org.au, phone our feedback line (07) 3826 1596, phone our office on (07) 3826 1500 or write to:

CEO
YFS Ltd.
PO Box 727
Woodridge QLD 4114

All complaints are dealt with in accord with the YFS complaints policy.

If you are not satisfied with the outcome of your complaint you may wish to contact the Office of the Australia Information Commissioner at www.oaic.gov.au