



# Privacy Policy

All sites

Policy Title & Code	Privacy Policy – All Sites – Administration – Organisational Integrity – 2020
Last edited by and on	Policy Manager – October 2020
Due for Review on	October 2023

# Privacy Policy

## **TABLE OF CONTENTS**

<b>1. Purpose .....</b>	<b>3</b>
<b>2. Scope .....</b>	<b>3</b>
<b>3. Principles.....</b>	<b>3</b>
<b>4. Policy Statements .....</b>	<b>3</b>
4.1 Information to be collected for a purpose .....	3
4.2 Manner of collecting personal information.....	3
4.3 Use of information .....	3
4.4 Information accuracy .....	4
4.5 Protection of personal and confidential information.....	4
<b>5. Guidelines .....</b>	<b>4</b>
5.1 Collecting personal information.....	4
5.1.1 Who the organisation collects personal information from.....	4
5.1.2 Type of information collected.....	5
5.1.3 How the organisation will collect personal information.....	6
5.1.4 Inform the person the information pertains to .....	9
5.2 Handling of personal information .....	10
5.2.1 Protect personal information .....	10
5.2.2 Storage .....	10
5.2.3 Transporting records .....	11
5.2.4 Accuracy .....	11
5.3 Accessing.....	12
5.3.1 Access to own personal information .....	12
5.3.2 Denying access.....	12
5.3.3 Access to employee records .....	13
5.4 Disclosing to third parties.....	13
5.5 Complaints .....	13
<b>6. Related documents and resources .....</b>	<b>14</b>
6.1 Legislation .....	14
6.2 Professional codes .....	14

---

6.3 Other external resources .....	14
6.4 Internal related policies.....	14
<b>7. Definitions .....</b>	<b>14</b>
<b>8. Version control.....</b>	<b>16</b>
8.1 Current .....	16
8.2 History .....	16
<b>9. Authorisation.....</b>	<b>17</b>

# Privacy Policy

## 1. Purpose

---

- The purpose of this policy is to ensure the **organisation**:
  - collects and manages personal information lawfully and according to the [Australian Privacy Principles](#) and other related laws
  - protects the personal information it holds from unlawful disclosure and misuse.

## 2. Scope

---

- This policy applies across all programs, services and activities falling under the umbrella entity of Youth Futures (**organisation**).
- Obligations under this policy apply to all staff, volunteers, students on placement and Board members of the **organisation**.

## 3. Principles

---

- The principles guiding this policy are:
  - the right to the confidentiality of personal information
  - accountability and transparency
  - integrity and respect for all.

## 4. Policy Statements

---

### 4.1 Information to be collected for a purpose

- The **organisation** will only collect [personal information](#) that is [reasonably necessary](#) to perform its functions and activities and meet its obligations.
- The **organisation** will not actively collect **personal information** that is unnecessary or irrelevant to its functions, activities and obligations.

### 4.2 Manner of collecting personal information

- The organisation will only collect **personal information** directly from the person the information pertains to, except if lawfully permitted otherwise.
- The **organisation** will collect personal information in a manner that is sensitive to the individual's capacity and circumstances.

### 4.3 Use of information

- The **organisation** will:
  - only use **personal information** for the purpose it was collected
  - inform the person in which the information pertains, the purpose for collecting personal information and the obligations in managing it.

#### 4.4 Information accuracy

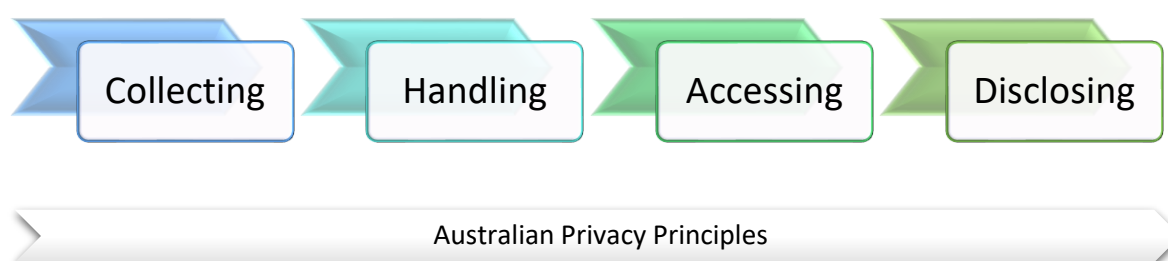
- The [organisation](#) will take reasonable steps to ensure the [personal information](#) it collects, uses or discloses is accurate, up to date and complete.

#### 4.5 Protection of personal and confidential information

- The **organisation** will protect **personal information** from misuse and not disclose it or allow access to a third party without consent, unless compelled or authorised by law.

## 5. Guidelines

These guidelines are set out under four phases of managing **personal information** - Collecting, Handling, Accessing and Disclosing (to third parties), based primarily on the [Australian Privacy Principles](#) that are relevant to the [organisation](#).



**Note:** [Employee records](#), that are directly related to a current or former employment relationship with the **organisation** are protected and can be accessed under workplace laws (i.e. employee records are not governed by the *Privacy Act 1988*).

### 5.1 Collecting personal information



#### 5.1.1 Who the organisation collects personal information from.

- The **organisation** may collect **personal information** about:
  - young people, or other family members of a young person who are seeking assistance from the organisation or are engaged with one of its programs, services or activities; for purposes including:
    - to determine eligibility for a service or program
    - to understand and respond to the service or program needs of young people
    - for funding and budget transparency, accountability and auditing
    - service and operational planning
    - to identify service gaps and improve service delivery
  - donors, contractors, suppliers and other stakeholders; for purposes including:

- business development and improvement
  - facility and contract management
  - ensuring supply of goods and services
  - fundraising
  - research
- o staff, students on placements and volunteers; for the purposes of recruiting and human resource management.

### 5.1.2 Type of information collected

- The **organisation** may collect **personal information** from young people and/or their parents/caregivers to enable the organisation to understand their needs in relation to housing, education or social support. This may include but is not limited to:
  - o mental and physical health history, current conditions or disability status
  - o educational history, achievements, capacities, or limitations
  - o personal, family and cultural background
  - o place and date of birth
  - o income, working status or history
  - o current housing status
  - o history of alcohol and drug use
  - o personal relationships of significance
  - o criminal history.
- Education programs are required to collect additional **personal information** when a young person enrolls, including immunisation status and previous school enrolled, as per the *School Education Act 1999*.

 For Registered Training Organisation see - *Policy 6 - Enrolment Policy*

 For Youth Futures Community School/Comet see - *Enrolment Policy*


 *School Education Act 1999.*

- Young people engaged with the **organisation** may disclose more sensitive and complex personal experiences to staff including details of traumatic events, abuse, emotional turmoil, or substance abuse. Staff must retain the confidentiality of these disclosures to the extent required of their professional codes of conduct and mandatory reporting for child sexual abuse.

 See *Preventing and Responding to Abuse of Young People Policy*.

 Code of Ethics for Youth Workers in WA.

 Australian Psychological Society Code of Ethics.

 Department of Education Code of Conduct.

### 5.1.3 How the organisation will collect personal information

#### 5.1.3.1 Collect from the individual

- The **organisation** will where reasonable and practicable collect **personal information** directly from the person the information pertains to, with their consent.
  - The **organisation** may collect **personal information** from a third party only if it is unreasonable or impracticable to collect it from the person concerned. The person the information pertains to may not be required to give consent in these circumstances, although it is preferred they give consent where possible.
    - A common example is when a referral is made for a young person by another person/agency to the **organisation**.
  - All reasonable steps will be made to inform a person if **personal information** is being collected about them from a third party, unless making that person aware would pose a serious threat to anyone's life, health or wellbeing.
  - The person the information pertains to should be informed as soon as possible what information was obtained, why and from who.

#### Unreasonable or impracticable?

Whether it is 'unreasonable or impracticable' to collect personal information directly from the individual concerned will depend on the circumstances.

Relevant considerations include:

- whether the individual would reasonably expect personal information about them to be collected directly from them or from another source e.g. a young person's personal information may be collected from a parent/caregiver
- whether direct collection from the individual would jeopardise the purpose of collection or the integrity of the personal information collected e.g. a job reference
- any privacy risk if the information is collected from another source
- excessive time and cost for collecting directly from the individual.

The following are examples of where it may be unreasonable or impracticable to collect personal information from the individual concerned and instead collect it from a third party:

- a document that is mailed to an individual is returned to the organisation so the individual's updated contact details may need to be obtained from someone else
- a young person lacks the capacity to give the required information.



**Source:** Australian Government – Office of the Australian Information Commissioner – *Australian Privacy Principles Guidelines - Chapter 3 - Collection of personal Information*

#### 5.1.3.1.1 If the personal information is sensitive

- **Sensitive personal information** should be collected directly from the individual the information pertains to, with their express consent.
  - **'Sensitive information'** is a subset of personal information and includes information or an opinion 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 orientation or practices, or
    - criminal record
    - health information about an individual
    - genetic information (*Privacy Act 1988 s. 6 (1)*)
  - **Consent** may not be required in certain situations to collect **sensitive information**. Examples include:
    - it is unreasonable or impracticable to obtain the individual's consent AND the sensitive information is needed to protect the life, health and safety of an individual or the public
    - the sensitive information is required or authorised by or under an Australian law or a court/tribunal order
    - the sensitive information is needed to take action for serious misconduct or unlawful activity that relates to the functions of the **organisation**
    - sensitive information is needed as part of a legal dispute. (*Privacy Act 1988 - S16A (1)* and Schedule 1 Australian Privacy Principle 3.4)

The above examples are the most relevant to the **organisation**. Further reasons for collecting **sensitive information** without consent can be found here:



*Australian Privacy Principles Guidelines – Chapter 3 – Collection of Personal Information*



### Personal v sensitive information

The *Privacy Act 1988* provides an additional level of protection for sensitive information which is why the rules for collecting it without consent are more stringent.

### Consent

Consent includes 'express consent or implied consent' (*Privacy Act 1988* s 6(1)). The four key elements of consent are:

- the individual is adequately informed before giving consent
- the individual gives consent voluntarily
- the consent is current and specific; and
- the individual has the capacity to understand and communicate their consent
- Express consent is given explicitly, either orally or in writing. This could include a handwritten signature, an oral statement, or use of an electronic medium or voice signature to signify agreement.
- Implied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the organisation.



**Source:** *Australian Privacy Principles Guidelines - Chapter B – Key Concepts*

#### 5.1.3.2 Recording of personal information

- Staff must record all personal information accurately and concisely using objective, factual, non-discriminatory and non-judgemental language.
  - Managers/principals are responsible for overseeing the quality of information relevant to their programs.

#### 5.1.3.3 Sharing personal between organisational programs

- Personal information provided to the organisation may be made available across all the programs and services within the organisation, where required.
  - Sensitive personal information however should not be shared across programs or services, unless the person the information pertains to has consented or one of the exceptions above apply (See 5.3.1.1 If the personal information is sensitive above)

#### 5.1.3.4 Manner of collection

- **Personal Information** will only be collected fairly.
  - Fairly means it will not involve intimidation or deception and is not unreasonably intrusive.
- It is preferred that **personal information** is provided via a written form or document signed by the person providing the information, or an email from their personal account.
  - If obtaining information in writing is not practical or reasonable, it may be provided verbally to staff who will record the information in writing. Staff should confirm the

record with the person providing the information who should then sign it as an accurate record of the information they provided.

- Information may also be confirmed by email exchange.
- Staff should only verbally collect personal information when in a quiet and private place, such as a closed office.
- A young person may have a parent/caregiver or other trusted third-party present to witness the collection of personal information; or who may provide the information on behalf of the young person.

### What would be fair or unfair?

What constitutes a fair way to collect personal information will depend on the circumstances. For example, it would usually be unfair to collect personal information secretly without the knowledge of the person concerned. However, this may be a fair means of collection if undertaken in connection with a fraud investigation.

'Unfair', would include:

- **collecting personal information from** an individual who is traumatised, in a state of shock or intoxicated
- collecting in a way that disrespects cultural differences
- misrepresenting the purpose or effect of collection, or the consequences for the individual of not providing the requested information
- collecting information by calling someone in the middle of the night.

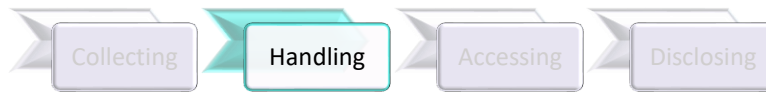


**Source:** *Australian Privacy Principles Guidelines - Chapter 3 - Collection of solicited personal information*

#### 5.1.4 Inform the person the information pertains to

- The **organisation** will inform the person the information pertains to, verbally or in writing, at the time the **personal information** is obtained, where relevant and practicable, the following details:
  - contact details of relevant person, position or office of the **organisation** for enquires
  - whether collecting the information is required or authorised by law
  - the purpose for collecting the information
  - the consequences if the personal information is not collected (e.g. unable to assess a person's eligibility for a program)
  - the type of circumstances where the information may be disclosed
  - that the organisation complies with relevant privacy laws and codes and this policy
  - they may access any personal information the organisation holds about them
- This information should be provided at the bottom of the relevant form or document, or during the verbal discussion.

## 5.2 Handling of personal information



### 5.2.1 Protect personal information

- The **organisation** will protect **personal information** it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure.
  - This includes protection from deliberate or inadvertent acts.
  - Staff will only access and use personal information held by the **organisation** for work related purposes as set out in this policy or the relevant law.
- **Sensitive (personal) information** will be given the highest protection.
  - Staff must not discuss or exchange **sensitive information** between each other about members of staff or young people, unless required for professional purposes or for the health, safety and wellbeing of another.
- Staff (including volunteers and students on placement) who misuse or breach the confidentiality of the **personal information** held by the **organisation** (except as permitted by law, this policy or a professional code of conduct) will be in serious breach of the Code of Conduct and may be terminated.

 See Youth Futures *Code of Conduct*.

### 5.2.2 Storage

- All records containing **personal information** must be kept on a secured drive, accessible by a password; or in a locked cabinet (for paper records) on organisational premises.
  - Records with personal information will only be accessible to authorised paid employees who need to access the information to perform their jobs.
  - Cabinets must be locked at the end of business each day, where relevant.
  - Personal information must not be left on display or unattended at any time.
  - Staff should not hold personal information of people associated with the **organisation** on a personal drive or with their own personal belongings or offsite, except for the purpose of transporting (see below [5.2.3 Transporting records](#)); or with the authorisation of their manager/principal or the CEO.
- Program managers/principles are responsible for authorising access for staff to the personal information they need and overseeing the security process.
  - Only managers/principals, the CEO and payroll staff may access [employee records](#).

 See also for the *Registered Training Organisation Policy 13 - Records Management Policy*.

### 5.2.3 Transporting records

- If personal records need to be transferred between site locations, staff must ensure they are transferred securely in a locked case, if possible.
  - The case/records should be transported in the boot of the vehicle (where available) and not be unattended at any time.
- If a staff member is transferring records at the end of the working day and needs to hold them overnight, the records must be kept securely at their residence, where they cannot be accessed by third parties.
  - Staff must not store records away from an [organisational](#) site for more than 3 consecutive nights during transit.
- Electronic files should be transferred via an email address of a person authorised to view the file, unless the record is too large.
  - Large electronic records can be transported via a USB, in a locked case as per the above process.
    - The records should be transferred and deleted from the USB as soon as they are transferred to the new device.

### 5.2.4 Accuracy

- Staff must ensure the [personal information](#) held by the **organisation** remains accurate, up to date and complete by regularly reviewing it.
- Education program managers/principals should review the personal information of young people held by the organisation annually.
- Staff must advise of any changes to their personal information to their manager/principal or the finance manager as they occur.

**Note:** The **organisation** may be subject to a fine under workplace laws if they make or keep employment records that they know are false or misleading. (*Fair Work Act 2009 s.535 and 536*)

 See *Fair Work Ombudsman website* (record keeping)

#### 5.2.4.1 Update incorrect personal information

- Any person may ask the **organisation** to update the personal information the organisation holds about them if they believe it is inaccurate, out-of-date, incomplete, irrelevant or misleading.
  - The request can be made in writing, via email or verbally for minor changes.

- For more extensive changes, requests should be confirmed in writing or email.
- Staff should comply with requests as soon as practicable, but within 10 working days.
- If a staff member reasonably believes the information being held is correct and should not be amended, they should advise the person in writing within 10 working days, giving the reason why the information will not be amended.

### 5.3 Accessing



#### 5.3.1 Access to own personal information

- Individuals may access the [personal information](#) the [organisation](#) holds about them.
- Requests for information may be made in writing, email or verbally.
  - Staff must confirm the identity of the person seeking the information before releasing it to them.
- Identity can be verified by staff who know the person or by providing photo identification or at least 2 other forms of identification with an address.
- Information should be provided within 10 working days, in the manner requested by the person where reasonable and practicable.
  - Information may be accessed by an individual by viewing the record or by staff providing an electronic or paper copy.
  - Staff must supervise people who are viewing their personal records to answer any further queries.
- The **personal information** of third persons in the record should be edited out before being released, unless the third party has consented to it being released to the person seeking the record.

#### 5.3.2 Denying access

- The **organisation** may deny access to someone's own **personal information** if:
  - releasing the information could pose a serious or immediate threat to the life, health or safety of an individual or public health or safety
  - releasing the information could have an unreasonable impact on the privacy of another person
  - the information relates to legal proceedings between the organisation and the individual (unless it is a formal request under those proceedings)
  - releasing the information could jeopardise or undermine a negotiation process, an investigation or law enforcement action.

The above reasons for denying access to personal information are the most relevant to the organisation under the *Privacy Act 1988*, however further reasons are available see:



*Australian Privacy Principle Guidelines Chapter 12 - Access to Personal Information*

### 5.3.3 Access to employee records

- An employee may access their own [employee records](#), during and after their employment has ended.
  - Personal information related to an employee, that are not '[employee records](#)'; and volunteers' personal records, will be treated as per the provisions above in '[5.3.1 Access to own personal information](#)'.
  - A person who has applied for employment at the [organisation](#) but was unsuccessful is covered by the provisions above in '[5.3.1 Access to own personal information](#)'.

## 5.4 Disclosing to third parties



- The [organisation](#) will only disclose personal information to a third party if:
  - the person the information pertains to has consented
  - it would be reasonably expected by the person the information pertains to, that a third party would need the information, for example, when providing a referral to a related service or in a health emergency
  - it is authorised by law or a court/tribunal
  - the organisation reasonably believes disclosure is required by an enforcement body, such as the police
  - it is to protect the life health and safety of a person
  - it is needed to take action for suspected unlawful activity or serious misconduct.
- Details of any disclosures made to a third party must be documented in the person's file with the **organisation**, including the reason for disclosure, what was disclosed, when and to who.
- If the person the information pertains to has not consented to the disclosure, the organisation will inform the person of the disclosure as soon as practicable, unless:
  - it will pose a real risk to the health safety and life of another person or
  - it will jeopardise any investigation by an enforcement body.

## 5.5 Complaints

- Complaints received by the **organisation** with regards to privacy issues will be dealt with in accordance with the *Grievance Policy*.

## 6. Related documents and resources

### 6.1 Legislation

 *School Education Act 1999*

 *Privacy Act 1988*

 *Fair Work Act 2009*

### 6.2 Professional codes


 Australian Psychological Society Code of Ethics.

 Code of Ethics for Youth Workers in WA.

 Department of Education Code of Conduct.


### 6.3 Other external resources

 Australian Privacy Principles – Quick Reference

 Australian Government – Office of the Australian Information Commissioner – *Australian Privacy Principle Guidelines*

 Fair Work Ombudsman website

### 6.4 Internal related policies

 *Preventing and Responding to Abuse of Young People Policy.*

 Registered Training Organisation - *Policy 6 - Enrolment Policy*

 Youth Futures Community School/Comet - *Enrolment Policy*

## 7. Definitions

**Australian Privacy Principles:** are legally binding principles which are the cornerstone of the privacy protection framework in the *Privacy Act 1988 (Cth)*. There are 13 Principles which set out standards, rights and obligations around:

- the collection, use and disclosure of personal information
- an organisation or agency's governance and accountability
- integrity and correction of personal information
- the rights of individuals to access their personal information.

(Source: Australian Government – Office of the Australian Information Commissioner – *Australian Privacy Principles*)

**Employee record:** means a record of personal information relating to the employment of the employee (not a volunteer). Examples include health information about an employee, as well as personal information relating to:

- engagement, training, disciplining, resignation or termination of employment
- the terms and conditions of employment
- the employee's personal and emergency contact details, performance or conduct, hours of employment or salary or wages
- the employee's membership of a professional or trade association or trade union
- the employee's recreation, long service, sick, maternity, paternity or other leave
- the employee's taxation, banking or superannuation affairs. (*Privacy Act 1988 s 6(1)*)

**Organisation:** any service, program or school falling under the umbrella entity of Youth Futures

**Personal information:** means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- whether the information or opinion is true or not; and
  - whether the information or opinion is recorded in a material form or not.' (*Privacy Act 1988 s.6.1*)
- Common examples are an individual's name, signature, address, telephone number, date of birth, medical records, bank account details, employment details and commentary or opinion about a person.
  - The following are the different types of personal information:
    - sensitive information
    - health information
    - credit information
    - employee record information and
    - tax file number information.

(**Source:** Australian Government – Office of the Australian Information Commissioners – *Australian Privacy Principle Guidelines - Chapter B - Key Concepts*)

**Sensitive information** – is a type of personal information which is given a higher level of protection and is defined as information or an 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 orientation or practices, or
- criminal record
- health information about an individual
- genetic information (that is not otherwise health information)
- biometric information that is to be used for the purpose of automated biometric verification or biometric identification, or
- biometric templates (*Privacy Act 1988 s 6(1)*).



- Sensitive information is given a higher level of privacy protection than other personal information. This recognises that inappropriate handling of sensitive information can have adverse consequences for an individual or others. For example, discrimination or mistreatment is sometimes based on a person's race or ethnic origin. Mishandling of sensitive information may also cause humiliation or embarrassment or undermine an individual's dignity.

(Source: Australian Government – Office of the Australian Information Commissioners – *Australian Privacy Principle Guidelines - Chapter B - Key Concepts*)

**Reasonably necessary:** The 'reasonably necessary' test is an objective test to determine whether a reasonable person who is properly informed would agree that the collection of personal information is required.

Factors relevant to determining whether a collection of personal information is reasonably necessary for a function or activity include:

- the primary purpose of collection
- how the personal information will be used in undertaking a function or activity (for example, in most circumstances collection on the basis that personal information could become necessary for a function or activity in the future, would not be reasonably necessary)
- whether the entity could undertake the function or activity without collecting that personal information, or by collecting a lesser amount of personal information.

(Source: Australian Government – Office of the Australian Information Commissioners – *Australian Privacy Principle Guidelines - Chapter 3 – Collection of Solicited Personal Information*)

## 8. Version control

### 8.1 Current

<b>This version</b>	Privacy Policy - July 2020
<b>Category</b>	All Sites – Administration – Organisational Integrity
<b>Date effective from</b>	01/10/2020
<b>Owner (Job title)</b>	Policy Manager
<b>Approval Authority</b>	CEO
<b>Review date</b>	October 2024

### 8.2 History

<b>Previous versions (number)</b>	<b>Effective dates (inclusive)</b>
External Privacy Policy (for website)	January 2015 -
Policy 20 - Privacy Policy	April 2013- October 2017

## 9. Authorisation

---

<b>Title</b>	CEO
<b>Name</b>	Mark Waite
<b>Date of approval</b>	29/09/2020