POLICY

Privacy

Youth Futures Community School Hubs - Community Schools, Anchor Point and Comet Connect

Policy title & category	School Governance - privacy
Last edited	Policy Manager – June 2025
Owner (job title)	CEO Youth Futures
Approval Authority	Board of Directors
Due for review	June 2026

Contents

Acknowledgement of Country

Youth Futures students, staff and parents/carers acknowledge and respect the Traditional Custodians of the lands and waters on which we live and are educated in Western Australia.

Privacy

1. Purpose

The purpose of this policy is to ensure YFCS Hubs:

- Comply with the amended **Privacy Act 1988** and the **Privacy and Other Legislation Amendment Act 2024**,
- Protects personal information from unlawful disclosure, misuse, or cyber threats and
- Responds transparently to requests and risks under the new privacy rights.

2. Scope

- This policy applies to all students enrolled at YFCS Hubs (Community Schools, Anchor Point and Comet Connect services) and
- Obligations under this policy apply to Board Directors, staff, volunteers and students on placement.

3. Principles

YFCS Hubs recognise and abide by the **Australian Privacy Principles**.

These principles are a set of thirteen legally binding principles under the *Commonwealth* Privacy Act 1988 that govern how most Australian public and private sector organisations handle personal information. They form the foundation of Australia's National Privacy Framework.

The thirteen Australian Privacy Principles (APPs) are:

1. **Open and Transparent Management**
   Agencies must manage personal information openly and transparently.
2. **Anonymity and Pseudonymity**
   Individuals should have the option to remain anonymous, where lawful and practicable.
3. **Collection of Solicited Personal Information**
   Only collect personal information that is necessary for functions or activities.

4. **Dealing with Unsolicited Personal Information**
   Reasonably determine whether to keep or destroy unsolicited personal information.

5. **Notification of Collection**
   Inform individuals about the collection and use of their personal information.

6. **Use or Disclosure of Personal Information**
   Use personal information only for the purpose it was collected unless an exception applies.

7. **Direct Marketing**
   Restrictions apply to the use of personal information for marketing purposes.

8. **Cross-Border Disclosure**
   Take reasonable steps to ensure overseas recipients do not breach the APPs.

9. **Adoption, Use or Disclosure of Government Identifiers**
   Limit use of government-issued identifiers (like Medicare or TFN) unless legally authorised.

10. **Quality of Personal Information**
    Ensure personal information is accurate, up to date and complete.

11. **Security of Personal Information**
    Protect personal information from misuse, loss, unauthorised access or disclosure.

12. **Access to Personal Information**
    Individuals have a right to access their personal information.

13. **Correction of Personal Information**
    Individuals have a right to request corrections to their personal information.

4. Policy statements

1. **Lawful and Limited Collection**
   Personal information is only collected when it is lawful and reasonably necessary for YFCS Hub functions, in accordance with APP 3 and APP 5.

2. **Fair and Transparent Collection Practices**
   Information will be collected fairly, with transparency about the purpose, legal basis and any potential consequences (APP 1, APP 3, APP 5).

3. **Use and Disclosure for Stated Purposes Only**
   Personal information will only be used or disclosed for the original stated purpose, or as authorised under APP 6 and APP 7.

4. **Right to Access and Correction**
   Individuals have the right to access their personal information and request corrections where it is inaccurate, outdated, incomplete or misleading (APP 12 and APP 13).

5. **Security and Protection of Information**
   YFCS Hubs implement reasonable steps—both technical and organisational—to protect information from misuse, loss and unauthorised access (APP 11).

6. **Restrictions on Cross-Border Disclosure**
   Personal information will not be shared overseas unless the receiving organisation upholds equivalent privacy protections (APP 8).

7. **Transparency in Automated Decision-Making (ADM)**
   Individuals will be informed when ADM processes are used and given the opportunity to seek a human review where the decision has a significant impact.

8. **Special Protections for Children and Sensitive Information**
   Additional safeguards are applied to information collected from children or where sensitive data (e.g. health, cultural background) is involved.

5. Definitions

Automated Decision-Making (ADM)
Processes using algorithms to make decisions without human involvement.

Data Breach
An incident where personal information is lost, accessed, disclosed or used without authorisation, which could result in harm to individuals.

De-identified Information
Data that has been stripped of personal identifiers and cannot reasonably be re-identified. Not subject to the same privacy protections as identifiable data.

Doxxing
Public release of identifying personal information with harmful intent.

Informed Consent
Freely given agreement to collect or use personal data, based on a clear understanding of what information is being collected, how it will be used, and the possible consequences.

Notifiable Data Breach (NDB) Scheme
A legal requirement under the *Privacy Act 1988* that mandates notification to the Office of the Australian Information Commissioner (OAIC) and affected individuals when a breach is likely to cause serious harm.

Personal Information
Any information or opinion about an identified individual, or an individual who is reasonably identifiable. This includes names, addresses, phone numbers, photos, school records and health information.

Privacy Collection Notice
A mandatory disclosure provided at the time of data collection explaining the purpose, legal basis, and rights relating to personal information collected.

Privacy Officer
The staff member responsible for ensuring privacy compliance, responding to access requests, and managing data breaches.

Sensitive Information
A subset of personal information that includes health records, racial or ethnic origin, political opinions, religious beliefs, sexual orientation or criminal records. It requires a higher level of protection under the Privacy Act.

Serious Invasion of Privacy
Intentional or reckless intrusion into personal life (now actionable in court).

Third Party
Any external person or organisation that is not part of Youth Futures (e.g. service providers, consultants, government agencies) and may receive personal information under permitted conditions.

6. Implementation

YFCS Hubs will implement the privacy policy in accordance with the Australian Privacy Principles and recent legislative amendments:

Lawful and Limited Collection:

- Staff must use YFCS Hub-approved data collection forms (only) that capture only what information is deemed necessary and
- Any new collection processes must be approved by the Principal or Policy Manager to ensure legal compliance.

Fair and Transparent Collection Practices:

- A *Privacy Collection Notice* (see definitions) must be provided verbally or in writing at the point of data collection and
- Staff must clearly explain why the data is being collected, whether it is required by law (or not), and what it will be used for.

Use and Disclosure for Stated Purposes Only:

- Staff must not repurpose or share personal information without documented consent, unless legally required to do so and

- Third-party disclosures must be logged on a dedicated YFCS Hub record with the date, recipient, type of information and reason for sharing.

Right to Access and Correction

- Requests for access or corrections to data collected must be forwarded to the Principal or Policy Manager for approval,
- The identify of the person seeking access or correction must be verified using a minimum of two approved forms of ID and
- YFCS Hub staff must respond to all requests within 10 working days and document the outcomes on a dedicated record.

Security and Protection of Information

- All YFCS Hub digital files must be stored on approved secure servers with password protection and encryption,
- All YFCS Hub paper files must be kept in locked storage when not in use,
- All YFCS Hub staff must complete annual privacy and data security training and
- All suspected information breaches must be reported immediately and managed under YFCS Hub's breach response protocol.

Restrictions on Cross-Border Disclosure

- Cross-border data transfers require written approval from the Principal or Policy Manager and
- All staff must confirm that overseas entities offer equivalent protection to Australian standards.

Transparency in Automated Decision-Making (ADM)

- When ADM is used, individuals must be informed in writing of the process, logic and implications,
- A designated YFCS Hub staff member must be available to provide human review upon request and
- ADM processes must be documented and reviewed annually for fairness and compliance.

Special Protections for young people and sensitive information

- For minors, staff must obtain parental/carer consent unless the young person is deemed mature enough to consent,
- Sensitive information e.g., trauma history should only be accessed by authorised YFCS Hub staff and
- All such information must be treated in accordance with professional codes of ethics and culturally responsive practice.

7. Breach response protocol

In the event of an actual or suspected privacy breach, the following steps must be followed without delay:

1. Contain the Breach

- If the breach involves doxxing or targeted disclosure, escalate immediately to the CEO and notify legal counsel,
- Otherwise immediately secure the data or system involved to prevent further loss or exposure and
- Notify the Principal or Policy Manager.

2. Assess the Breach

- The Principal or Policy Manager will assess the type, sensitivity and scope of the breach and
- Determine whether the breach is likely to result in serious harm to any individual.

3. Notify Affected Parties

- If serious harm is likely, notify affected individuals as soon as practicable and
- Notify the **Office of the Australian Information Commissioner** in accordance with the Notifiable Data Breaches (NDB) scheme.

4. Containment and Recovery

- Take steps to limit further impact e.g. revoke access, change passwords, isolate affected systems and
- Engage IT support and legal counsel if required.

5. Review and Prevent Recurrence

- Conduct a post-incident review to identify causes and process failures and
- Implement improvements such as system upgrades, staff training or policy changes.

6. **Documentation and Reporting**

Maintain a detailed breach register including:

- Date/time of breach,
- Nature of the breach,
- Steps taken,
- Notification details and
- Lessons learnt.

7. Related documents and resources

Commonwealth Privacy Act 1988

Commonwealth Fair Work Act 2009

WA School Education Act 1999

Commonwealth and other legislation Act 2024

8. Review process

YFCS Hubs are committed to continuous improvement and will undertake annual reviews of policies and procedures informed by the following approach:

- Establish a review framework,
- Assemble a review team,
- Gather 360-degree feedback from multiple sources i.e. students, parents/carers, teaching and key stakeholders from within and outside of YFCS Hubs,
- Analyse incident and practice data for systemic trends,
- Draft revisions to the existing policy and procedures and share widely for input,
- Obtain endorsement from the CEO and Principal,
- Communicate changes to all staff (and provide additional training where relevant) and
- Implement and monitor the updated policy.

9. Version control

9.1 Current

This version	Privacy
Category	Youth Futures Community School
Date effective from	June 2025
Developed by	Policy Manager Youth Futures
Owner (Job title)	Principal – YFCS Hubs
Approval authority	CEO Youth Futures
Review date	June 2026

9.2 History

Previous versions	Effective dates
Privacy Policy	2020
External Privacy Policy (for website)	2015
Policy 20 - Privacy Policy	2013