

POLICY 1.1 - PRIVACY & CONFIDENTIALITY

Background Information

Wonderland Community Services (WCS), operating across two states, is committed to upholding:

- **Commonwealth Privacy Act 1988**
- **Personal Information Protection Act 2004 (Tas)**
- **Information Privacy Act 2009 (Qld)**

While WCS is not a government agency, it operates under the regulatory standards of the **Department of Health and Human Services** and the **NDIS Commission**.

Policy

WCS is legally and ethically required to protect the personal and confidential information of all individuals associated with its services, including participants/young people, families, carers and staff. All information must be managed in a way that prioritises the safety, wellbeing and protection of children and young people from harm, exploitation or unauthorised identification.

Failure to comply with this policy may place participants/young people at risk and will be treated as a serious breach, which may result in disciplinary action, including termination of employment.

Scope of Confidential Information

Confidential information may include, but is not limited to:

- Participant/young person's location
- Funding information
- Disability and medical records
- Records of past trauma
- Police history
- Any personal information shared verbally or in writing
- Electronic records and associated data that may identify a participant/young person

Procedure

1. Verbal & Written Communication

Confidential information must not be shared without prior written consent, except where outlined in this policy. This includes:

- Verbal sharing with others in the community
- Written sharing (emails, messages, notes) with unauthorised persons

Note: WCS requires written permission (via consent forms) during the intake process and prior to signing an Individual Service Agreement. This ensures appropriate information sharing with other service providers and support personnel.

Staff must ensure that communication involving children and young people is handled with additional care to prevent harm or identification.

2. Exceptions to Consent Requirement

Confidential information may be disclosed without prior consent:

- In medical or safety emergencies (to medical staff, police, or child safety workers)
- Internally, to other WCS staff involved in a participant/young person's care (all staff are bound by this policy)
- To WCS management for decision-making
- To the NDIS Commission in the event of a reportable incident

Any disclosure must be proportionate, limited to the minimum information necessary, and directly related to the safety, wellbeing or legal requirements of the participant/young person.

3. Use of Artificial Intelligence (AI)

WCS recognises that Artificial Intelligence (AI) tools may support administrative tasks; however, their use presents risks to privacy, confidentiality and the safety of the participant/young person.

Permitted Use

AI may only be used:

- For administrative support tasks
- To improve structure, formatting and grammar of documentation
- Using fully de-identified information only

Conditions of Use

Staff must ensure:

- Use is approved by management or aligned with organisational expectations
- AI is accessed only through approved systems where applicable
- AI is used as a support tool only, not a decision-maker
- All outputs are reviewed, edited and approved prior to use
- Professional judgement is always applied

Prohibited Use

Staff must not:

- Enter identifiable participant/young person information into AI systems
- Use names, locations or identifying details
- Upload or copy full incident reports, case notes or raw documentation
- Use AI for clinical, behavioural or risk-related decision-making

Risk and Confidentiality

AI systems operate on external platforms outside WCS control. WCS cannot guarantee how information is stored, processed, or retained. Use of AI must not compromise the safety, rights, or wellbeing of the participant/young person.

Accountability

All staff remain responsible for:

- Accuracy of AI-assisted work
- Appropriateness of content
- Maintaining confidentiality

Misuse of AI will be treated as a serious breach of this policy.

Staff Privacy and Confidentiality

WCS applies the same high standards of privacy to all staff:

- Staff sign a **Confidentiality Commitment Form** during onboarding and again bi-annually
- All personal and employment-related information is stored securely in the **Employee WCS Board**, accessible only to HR and senior management
- Staff photos/videos are only used with signed consent forms
- Staff must delete participant/young person photos/videos from personal devices (e.g., WhatsApp) after uploading them to official platforms (Care Boards/Case Notes)

Staff must maintain heightened awareness when handling information relating to children and young people.

Implementation Documents

WCS supports this policy using the following:

1. **Confidentiality Commitment Form**
2. **Permission Forms** (including Release of Information and Media Consent)
3. **Everyone is Important** induction presentation

Social Media & Media Use

Media content (photos/videos) is used to promote a sense of community, celebrate achievements, and build relationships. However:

- No surnames or identifying information will be included in social media captions
- Participants/young people and their families must provide prior written consent
- Media taken on personal phones must be deleted after official upload

Content must not allow a child or young person to be identified directly or indirectly, including through location, context, or repeated exposure. Additional care must be taken to ensure that children and young people cannot be identified or placed at risk through media content.

Confidentiality Breaches

A breach includes any unauthorised access, use, disclosure, or loss of information.

All breaches must be reported immediately to the Site Manager.

WCS will:

- Assess the severity and risk of harm
- Take immediate action to mitigate risk
- Notify relevant authorities where required
- Implement corrective actions

WCS promotes a no-blame reporting culture to encourage transparency; however, all staff remain accountable for their actions.

Failure to report or intentional misuse of information may result in disciplinary action.

Record Keeping

Records must be stored within approved organisational systems such as:

- **Records of Conversation:** Stored on MONDAY.COM → DOCUMENTS
- **Incident Reports:** Uploaded to MONDAY.COM → INCIDENT & FIRST AID REPORTS

Notifiable Persons

All concerns must be reported to the Team Leader, who will escalate to the Site Manager where required.

Information Sharing Without Consent

Information may be disclosed without consent only:

- As required by law or court order
- In response to legitimate requests from:
 - NDIS Commission
 - Australian Tax Office
 - Centrelink
 - Fair Work Ombudsman
 - Law enforcement agencies

Information sharing must be limited to what is necessary and must prioritise the safety and protection of the participant/young person.

In such cases, HR will manage communication and ensure only necessary information is disclosed.

Continuous Improvement

- Concerns or suggestions are to be directed to the HR Officer or Management Team
- Weekly management meetings will address emerging issues
- Compliance and Safety Officers will assess and mitigate privacy-related risks as part of WCS's **Risk Management Strategy**
- WCS will continue to review practices to ensure alignment with best practice in protecting children and young people.

DATE	PERSON/S	DETAILS
23.04.2026	Seonu Paek	Review and update
31.07.2025	Becci Fazldeen	Review and update
20.01.2025	Ashleigh Davis	Review and update
14.12.2023	Bronwyn McMullen	Review and update