

POLICY 1.7 – DATA MANAGEMENT POLICY

Purpose and Scope

This policy outlines WCS's commitment to safeguarding personal information in accordance with relevant state, federal, and sector-specific laws and standards. It applies to all staff, volunteers, participants/young persons, families, carers, and stakeholders involved with WCS.

Legislative and Regulatory Framework

WCS is committed to upholding the following legal and regulatory frameworks:

- Commonwealth Privacy Act 1988
- Personal Information Protection Act 2004 (TAS)
- Information Privacy Act 2009 (QLD)
- NDIS Practice Standards (2021) – as a registered NDIS provider
- Human Services Quality Framework (HSQF) – as a child safety provider

Definition of Personal Information

Personal data refers to any information that identifies or could reasonably identify a participant/young person, family member, carer, or staff member. This includes, but is not limited to:

- Location details
- Funding levels
- Disability and medical information
- Records of trauma
- Police or legal history
- Any spoken, written, or observed information

Types of personal information may include:

- Spoken Information: Verbal disclosures made directly or in presence of WCS staff
- Written Information: Information recorded in hardcopy or digital form, either created by or transferred to WCS
- Incidental Information: Observations made by staff (e.g., conditions at home during pickups)

Staff Responsibilities and Obligations

All WCS staff, contractors, and volunteers must:

- Sign the Staff Confidentiality & Safety Commitment Form and WCS Code of Conduct during induction.
- Uphold this Data Management Policy at all times.
- Not disclose personal information to any third party without prior written consent.

Permissible Disclosures

Information may be disclosed without consent in the following circumstances:

- Emergencies involving medical, police, rescue, or child safety services
- Internal care needs to other staff for continuity of service
- WCS management for decision-making and oversight
- NDIS Commission in reportable incident cases
- Legal requirements under court order or subpoena

Communicating this Policy to Participants

WCS will explain confidentiality policies to each participant/young person during induction, using the language and communication style best suited to their understanding. This policy will be made available:

- On WCS's official website
- Upon request in a variety of accessible formats

Information Storage, Access & Security

WCS ensures that all data is managed using secure and appropriate systems:

- **Digital Storage:** Information is stored on secure work laptops protected by antivirus/internet security software and secure third-party platforms (e.g., Monday.com).
- **Access:** Limited to staff with secure personal logins. No documents are to be downloaded to personal devices.
- **Record Retention:** Participant/young person records are securely retained for 7 years after disengagement from WCS. Access may be requested by the participant or nominated representatives, with WCS committing to respond within seven business days.
- **Smartphone Usage:** Any photos taken of participants on personal devices must be deleted at the end of the shift.

Data Sharing and Communication

Where appropriate and with consent:

- Support plan details may be shared with families, carers, service providers, or government agencies.
- Information sharing occurs during transitions to or from WCS as outlined in the participant's service agreement.

Amending or Updating Information

- Staff may update their personal data via FoundU or Monday.com, or by contacting WCS administration.
- Participants/Young Persons (or their representatives) may update details via online forms on WCS websites or after events like NDIS reviews.

Use of Social Media

- WCS may use images taken during activities for feedback or promotional purposes only if the Permission to Photograph, Video and Post on Social Media form has been completed and signed.
- Photos may be shared via WhatsApp between staff and management.
- Participants/young persons (or their representatives) have the right to withdraw consent at any time, and WCS will remove any associated media promptly.
- Identifying information (e.g., last names or locations) will never be shared alongside posted content.

Breaches of Privacy

WCS acknowledges that breaches may occur unintentionally. Staff are encouraged to report any suspected breaches to their Site Manager immediately.

Responses to a breach may include:

- Apology and acknowledgment to the affected party
- Participation in mediation or resolution processes
- Disciplinary action, including dismissal in serious cases

WCS management will:

- Assess the breach and its severity
- Determine safety risks
- Take steps to mitigate harm (including escalation where necessary)
- Review and improve internal procedures
- Deliver staff training if gaps are identified

Record Keeping

WCS maintains detailed records of:

- Conversations: via Record of Conversation (JotForm on WCS App and Monday.com)
- Incidents: via Incident Reports (uploaded to Monday.com under *Incident & First Aid Reports*)
- Notifications: directed to Team Leader → Site Manager

Related Documents and Forms

- Staff Confidentiality & Safety Commitment Form
- Consent Forms:
 - Permission to Obtain and Release Information
 - Permission to Photograph, Video and Post on Social Media
- Participant/Young Person Rights Policy
- “Everyone is Important” PowerPoint resource

These documents support the implementation of this policy and are freely accessible on the WCS website.

DATE	PERSON/S	DETAILS
01.08.2025	Becci Fazdeen	Review and update
20.01.2025	Ashleigh Davis	Review and update
23.10.2024	Cita Carmody-Pearson	Review and update