



Privacy, Confidentiality & Record-Keeping Policy

Policy Statement:

Pennant Hills Before and After School Care Service will make every effort to protect the privacy and confidentiality of all individuals associated with the service by ensuring that all records and information about individual children, families, educators, staff and management are kept in a safe and secure place. We ensure the appropriate use, storage and disposal of all records. Information will not be divulged or communicated, directly or indirectly, to another person unless necessary for maintaining the safety and wellbeing of a child.

Definitions:

Personal Information: Information or an opinion about an identified individual, or an individual who is reasonably identifiable.

Sensitive Information: A subset of personal information that includes details about a person's health, medical conditions, allergies, cultural background, family circumstances, disability, or any information relating to a child's safety, welfare or wellbeing. Sensitive information requires a higher level of protection and restricted access.

Privacy: The fundamental right of children, families and staff to have their personal, sensitive and health information protected from misuse, unauthorised access or disclosure.

Confidentiality: The professional obligation to keep children's and families sensitive, personal and health information private, secure and only accessible to authorised individuals.

Disclosure: The act of sharing personal, sensitive or health information about a child, family member, educator or staff member with another person or organisation. This may occur verbally, in writing or through digital communication, and must only happen when it is necessary for the safe operation of the service, required to support a child's wellbeing, or permitted or mandated under legislation such as child protection laws.

Data Breach: Any unauthorised access, disclosure, loss or misuse of personal or sensitive information. A breach may be accidental or deliberate and may involve physical documents, digital systems or verbal communication.

Considerations:

- Privacy Act 1988 (Cth)
- Children Legislation Amendment Act 2009 (NSW)
- Australian Child Protection Legislation and Leadership Framework
- Child Safe Standards (NSW)
- Education and Care Services National Regulations (2011)
 - Regulation 168(2)(l) - Services must have policies and procedures on records and information management.
 - Regulation 181 - Confidentiality of records and information.
 - Regulation 182 - Storage of records and access to records.
 - Regulation 183(2) - Retention periods for records (children's records, staff records, incident and illness records, etc.).
- Education and Care Services National Law (2010)
 - Section 12 - Responsibilities of the Approved Provider
 - Section 21-22 - Responsibilities of the Nominated Supervisor
 - Section 161A - Offence to fail to provide required information
 - Sections 174-176 - Offences related to notification and prescribed documentation
 - Section 188 - Protection from liability
- National Quality Framework:
 - Element 4.2.2 - Professional standards guide practice, interactions and relationships
 - Element 7.1.2 - Management systems
 - Element 7.1.3 - Roles and responsibilities
 - Element 7.2.3 - Development of professionals
- Australian Child Protection Legislation and Leadership
- Young Person (Care & Protection) Act 1998

Policy:

Confidentiality, Disclosure & Breaches:

Confidentiality Obligations:

On commencement of employment, all staff are to sign a confidentiality agreement and receive induction training where they learn expectations for handling personal, sensitive and health information. This training emphasises that confidentiality in verbal communication, written communication, and digital systems must be maintained at all times.

Permitted Use & Disclosure:

In certain circumstances, legal requirements, usually in relation to child protection, supersede the limits of confidentiality. In these cases, private information may be disclosed to regulatory

authorities, if it pertains to the safety of a child. In these cases, consent is not required to share information.

Staff may share information with government and non-government agencies under Chapter 16A of the Children and Young Persons (Care and Protection) Act 1998. Any information sharing of this nature should be documented appropriately and securely.

Particularly sensitive and confidential information is stored on password-protected drives that are only accessible by the Nominated Supervisors. Multi-factor authentication is used for email access, and computers are regularly checked to ensure compliance.

Managing & Preventing Breaches:

1. If a suspected data breach occurs, the Approved Provider/Nominated Supervisor will undertake a reasonable and expeditious assessment to determine if the breach is likely to result in serious harm to any individual affected.
2. Individuals at likely risk of serious harm will be notified promptly.
3. The Approved Provider/Nominated Supervisor will access The Australian Government – Office of the Australian Information Commissioner website for more information.
4. Depending on the type and severity of the breach, a plan will be developed and all relevant parties notified of actions to be taken.
5. A post-incident review will be undertaken to assess what preventative actions can be taken.

All staff are responsible for accessing, storing and sharing private information appropriately and with care. Staff are also responsible for notifying centre management as soon as possible when a breach is suspected or discovered.

Families or staff who have concerns about privacy, confidentiality or record keeping may raise a complaint following the service's Management of Complaints Policy.

Records Management:

Record Types:

- Child enrolment and attendance records
- Medical, health, allergy and risk management records
- Incident, injury, trauma and illness records
- Staff records (qualifications, WWCC, training certificates)
- Programming documentation and staff communication records
- Financial and administrative records
- Digital records stored in childcare software and cloud systems

Collection of Information:

All information regarding the children and families attending the service is to be used solely for the purposes of providing childcare and meeting the administrative requirements of operating the service.

Consent from families will be obtained through enrolments, permission slips, notes and emails. Consent is sought on enrolment before taking images and videos of children. For more information on authorisation, please see our Acceptance & Refusal of Authorisations Policy.

All digital content, such as photos and videos, is stored securely and access is limited to authorised personnel only.

Access to Information:

Parents and guardians may access their child's information upon request, and staff may access their own employment records. All requests must be submitted in writing to the Approved Provider or Nominated Supervisor. In NSW, Information Exchange provisions also allow authorised agencies and non-government organisations to share information relevant to a child or young person's safety, welfare, or wellbeing.

Information held by the service is otherwise kept confidential and only shared when necessary to support a child's medical or developmental needs, when required by the Department of Education or an authorised officer, or when permitted under legislation. Access may be limited in circumstances such as court orders or safety concerns. Where access is disputed, individuals should follow the complaints pathway as outlined in the Management of Complaints Policy.

Data Security & Storage:

Physical Security:

All confidential physical records are stored in locked filing drawers with restricted access. Staff are required to ensure secure handling of documents during program hours (i.e. ensuring the proper storage and filing of documents used throughout the session).

Digital Security:

Our Childcare Software Provider assigns role-based access so that each user can only view or manage information appropriate to their responsibilities. Service information must not be stored on personal devices; however, in an emergency such as a power outage, staff may temporarily access the system on their own device to ensure attendance records are accurately maintained.

Qualified IT professionals support the service by keeping all digital systems secure and up to date. Further information is available in our Safe Use of Digital Technology & Online Environments Policy.

Retention & Disposal of Records:

The Nominated Supervisor is responsible for ensuring the correct archiving of documents for the minimum retention periods as laid out in Regulation 183 of the Education and Care Services National Regulations. This applies to:

- Child attendance and enrolment records
- Incident, injury, trauma and illness records
- Staff records
- Financial and administrative records

The Nominated Supervisor ensures that documents ready for disposal will be double-checked and approved before being disposed of appropriately (e.g. shredding hard copies, secure deletion of digital files).

Third-Party Systems & Data Sharing:

We ensure all third-party systems comply with the Australian Privacy Act 1988, guaranteeing that sensitive, personal, and financial data is handled securely, with ISO27001 compliant storage, strict access controls, and data encryption. Data is primarily used for Child Care Subsidy (CCS) management and, with consent, for tracking children's developmental and health information.

When engaging with any third-party systems, the centre ensures they meet all regulatory requirements, complying with the National Quality Framework. Systems need to integrate seamlessly with government portals and other childcare management tools. They must also incorporate automatic updates to reflect changing regulations.

Version	Action	Date
V.1	New policy created that pulled information from numerous other policies about: - Confidentiality responsibilities - Record-keeping - Information sharing - Third-party systems	28 th January 2026
V.1	Approved by PMC	18 th February 2026