Privacy and Confidentiality Policy

Document Title	NQS7.60 Privacy and Confidentiality Policy	Version	3a
Date Approved	January 2024	Date for Review	August 2024
Warning - Ensure you are using the latest version of this policy.			
DCC Network/All Organisation Information/DCC Policies/Quality Area 7 – Leadership & service management			

1. Policy Statement

Deniliquin Children Centre cares about your privacy and is committed to protecting your personal information in accordance with this policy and the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth) – which also includes the Australian Privacy Principles ('APP's'). The purpose of this privacy notice is to set out the type of information that we may collect about you and the purposes for which we will use and/or disclose your personal information and how it should be treated.

2. Rationale

This policy is to address the issues of privacy and confidentiality of children, families, educators, volunteers and committee of the service. It aims to protect the privacy and confidentiality by ensuring that all records and information about individual children, families, educators and management are kept in a secure place and are only accessed by or disclosed to those people who need the information to fulfil their responsibilities at the service or have a legal right to know.

3. Responsibilities

It is the responsibility of the Approved Provider to:

- Ensure that each family, staff, volunteers and student and board member is provided with a privacy collection statement upon enrolment, that includes details about how they can access their personal information, have this corrected as needed, make a complaint about a breach of privacy, if one occurs.
- Ensure each staff member, board members, volunteers and student information is correct in personnel and other files. This includes information on qualifications, WWCC, criminal history checks, staff entitlements, contact and emergency information, health and immunisation information, and any relevant medical and legal information. This would include any other relevant information collected by the service.
- Ensure that information collected from families, educators, board members and the community is maintained in a private and confidential manner at all times.
- Ensure that such information is not divulged or communicated (directly or indirectly) to another person other than the ways outlined as appropriate in the Education and Care Services National Regulations, 181, which says information can be communicated:
    - to the extent necessary for the education, care or medical treatment of the child,
    - to the parent of the child to whom the information relates (except for information in staff records),
    - to the regulatory authority or an authorised officer,
    - as authorised, permitted or required to be given by or under any act or law, and
    - with written consent of the person who provided the information.

- Ensure families are informed upon enrolment how images/photographs of their children will be used on the Internet and/or publications and gain written approval.
- Provide families with information on the Complaints and Feedback procedure if any privacy or confidentially procedure has been breached. Individuals can make a complaint to the Approved Provider if they believe there has been a breach of their privacy in relation to the Privacy principles. The breach will be assessed by the Approved Provider within 14 days. Where the information collected is incorrect, the information will be corrected. Where a serious breach of privacy is found, appropriate actions will be negotiated between the Approved Provider and the individual to resolve the situation, in line with the Feedback and Complaints policy.
- Ensure information provided by families, staff and board members is only used for the purpose it was collected for.

It is the responsibility of nominated supervisors to:

- Ensure each families' information is correct in enrolment records. This includes information on immunisation updates, income and financial details (credit card or bank information), contact details of family and emergency contact information, children's developmental records, Family Assistance information, and any medical or legal information – such as family court documentation – required by our education and care service. This would include any information required to be recorded under the National Law and Regulations, the Family Assistance Law and other relevant information collected to support the enrolment of a child.
- Provide families with details on the collection of personal information collected. This information will include:
    - the types of information collected by our education and care service;
    - the purpose of collecting information;
    - what types of information will be disclosed to the public or other agencies; and when and why disclosure may occur;
    - how information is stored at the service;
    - approaches used to keep information secure;
    - who has access to the information;
    - the right of the individual to view their personal information;
    - the length of time information needs to be archived; and
    - how information is disposed of.
- Ensure information provided by families and staff is only used for the purpose it was collected for.

It is the responsibility of employees to:

- Maintain children's information and store documentation according to policy at all times.
- Not share information about the education and care service, management information, other educators or children and families, without written permission or legislative authority.
- In keeping with the Early Childhood Australia (ECA) Code of Ethics (2008), the Education and Care Services National Regulations and the Privacy Legislation, respect the privacy rights of children enrolled and their families; educators and staff and their families and any other persons associated with the service.
- Sign a Confidentiality Statement as it relates to privacy and confidentiality of information.

4. Definitions

Nil

5. Guidelines

We will

- Maintain private and confidential files for staff members, children and their families.
- Develop systems for the appropriate use, storage and disposal of records.
- Ensure the information in these files is used only for the education and care of the child enrolled in the service, and only shared with relevant or authorised people as defined within authorisations of the Education and Care Services National Regulations.

Our education and care service aims to meet these goals through the adoption of this specific Privacy and Confidentiality policy and our Privacy Collection statement which will guide our practices in this area.

a) Storage of Information

Ensure that education and care service records, personnel records, CCS information and children's and families information is stored securely reducing the chance of unauthorised access, use or disclosure and remains private and confidential within the education and care environment at all times.

River Region Early Education will ensure that up to date computer virus protection technology, and other appropriate technology such as password security protocols to exclude unauthorised access.

b) Security of personal information

The Approved Provider or Nominated Supervisor will take reasonable steps to protect personal information from misuse, interference and loss, unauthorised access, modification or disclosure.

These steps include:

- Taking responsibility for the security of personal information and regularly checking the practices implemented to protect it. This will include management of access privileges to ensure only people who genuinely need to see personal information can access it.
- Ensuring information technology systems have appropriate security measures including password protection, anti-virus and 'malware' software, and data backup systems.
- Ensuring physical repositories of personal information are secure, in a locked filing cabinet in the Nominated Supervisor, Finance Manager and General Managers office.
- Ensuring all educators and staff are aware of their obligations in relation to the collection, use and disclosure of personal information, through activities like mentoring, staff meetings or on-line training courses.
- Requiring all educators, staff, volunteers and work experience students to sign a 'Confidentiality Statement' acknowledging that personal information:
    - can only be accessed if it is necessary for them to complete their job
    - cannot be disclosed to other organisations (including colleges, RTOs) or discussed with individuals outside the service including personal family members unless they have written consent from the person (or parent) concerned.
    - must be stored in compliance with service practices which safeguard its security.

- Ensuring records which we don't need to keep, including unsuccessful job applications and records which fall outside the record keeping timeframes under the National Education and Care Law and Regulations (refer to our Record Keeping and Retention Policy) are destroyed in a secure way as soon as possible by, for example, shredding, incinerating or permanently deleting electronic records including archived or back-up copies. Where possible, the destruction of records containing personal information will be overseen by two staff members.
- Ensuring employees and other relevant persons only have access to the personal information required to do their job
- De-identifying personal information which may come into the public domain. For example, removing identifying names or details from newsletters etc.
- Ensuring staff comply with our *NQS7.61 Accessible Use of Electronic Media Policy* (for example by obtaining authorisation from a child's parents before posting any photos of their child on the Service social media page, and not posting personal information on any social media page which could identify children or families.)
- Ensuring confidential conversations with parents or with staff are conducted in a quiet area away from other children, parents and staff.

c) Breaches of Personal Information

The Approved Provider or Nominated Supervisor will implement the Service's Data Breach Response Plan and notify individuals and the Australian Information Commissioner (the Commissioner) if personal information is lost (hard copies or electronic), accessed or intentionally/unintentionally disclosed without authorisation, and this is likely to cause one or more persons serious harm.

Data Breach Response Plan

Employees must notify the Approved Provider or Nominated Supervisor about a breach or suspected breach of personal data as soon as they suspect the breach or become aware a breach has occurred. The Approved Provider or Nominated Supervisor will:

- quickly assess the situation to decide whether or not there has been a breach. This assessment must be completed within 30 days but given the potential for serious harm to individuals, should be completed as soon as possible.
- record the nature of any data breach, and the steps taken to immediately contain the breach where possible and ensure it does not happen again. If necessary, they will contact external experts for advice and guidance, for example on cybercrime (hacking) and information technology security measures like access, authentication, encryption and audit logs
- notify the Commissioner and the individuals where there is a risk of serious harm after a data breach
- liaise with their insurer to determine whether the insurance policy covers data breaches and any steps they need to take
- evaluate the effectiveness of their response to the data breach and implement improvements to the Plan if required after all notifications, records and remedial action are taken.

Serious harm

The Approved Provider or Nominated Supervisor will decide whether serious harm of a physical, psychological, emotional, financial or reputational nature is likely once fully informed about the

type and extent of the breach. They will consider the type and sensitivity of the information, the type of security protecting the information if any (e.g. encryption) and how likely it is the information will be used to cause harm to individuals. Examples of the kinds of information that may increase the risk of serious harm include sensitive information like an individual's health records, documents commonly used for identity fraud e.g. Medicare card, birth certificates and financial information.

The Approved Provider or Nominated Supervisor will also consider how long the personal information has been accessible because serious harm is more likely the longer it has been since the data breach.

Where a data breach occurs, there may be not always be a risk of serious harm. This may be the situation, for example, if a trustworthy person or organisation who has received personal information in error confirms they have not copied, and have permanently deleted the information, or where expert advice states it's unlikely encrypted data can be accessed.

Where they are satisfied there is no risk of serious harm, the Approved Provider or Nominated Supervisor are not required to notify individuals or the Commissioner about the breach. They may choose to advise the individuals concerned about the breach and the action taken. The Approved Provider or Nominated Supervisor will however appropriate keep records about the breach.

Notifying the Commissioner

Where there is a risk of serious harm after a data breach, the Approved Provider or Nominated Supervisor will prepare a Statement for the Commissioner which includes the name and contact details of the Approved Provider or Nominated Supervisor, a description of the data breach (including date occurred and detected and who obtained information), the type of information involved (why it may cause serious harm), and the steps individuals at risk of serious harm should take in response to the breach (e.g. steps to request new Medicare card or credit card). The Approved Provider or Nominated Supervisor will get specialist advice about the recommended steps if required. They may use the Notifiable Data Breach Form available online from the *Office of the Australian Information Commissioner* to notify the Commissioner.

Notifying Individuals

Where there is a risk of serious harm after a data breach, the Approved Provider or Nominated Supervisor will notify individuals about the breach as soon as possible using the most appropriate communication methods for the individuals concerned e.g., a telephone call, SMS, physical mail, social media post, or in-person conversation. The information provided is the same as that required for the Commissioner. It might also explain steps the Service has taken to reduce the risk of harm to individuals. The Approved Provider or Nominated Supervisor may notify everyone whose personal information was part of the breach or only those individuals at risk of serious harm. If this is not possible or practical, they may publish a copy of the Statement, for example on their website or Facebook page, and take steps to ensure individuals at risk of serious harm see the publication.

d) Access to Information

The Nominated Supervisor will ensure that information kept is not divulged or communicated, directly or indirectly, to anyone other than:

- medical and developmental information that is required to adequately provide education and care for the child, or
- the Department of Education and Communities, or an authorised officer, or

- as permitted or required by any Act or Law.
- individuals will be allowed access to their personal information when they request it. Authorised persons may request to view any information kept on their child.

Every enrolling parent/guardian is provided with clear information in the enrolment form about:

- what personal information is kept, and why.
- any legal authority to collect personal information.
- third parties to whom the service discloses such information as a usual practice.

Information may be denied under the following conditions:

- access to information could compromise the privacy of another individual;
- the request for information is frivolous or vexatious;
- the information relates to legal issues, or there are legal reasons not to divulge the information such as in cases of custody and legal guardianship.

This is not an exhaustive list of circumstances where we may be entitled or even required to deny access to information.

e) Information we collect about you

Details about the information we collect and why can be found in the privacy collection statement.

f) Information on Display.

Persons who enter River Region Early Education services may be able to view some information about the children in our care there, for example photos or artwork which may divulge the child's name and age. In some cases it may be necessary to have on display health information so that we can have ready access to it for emergency purposes.

The Nominated Supervisor will ensure information provided by families and staff is only used for the purpose it was collected for.

g) Updating of Information

The service will request updates of this information annually, via the Enrolment update form, or when a change occurs in the child's medical or personal details.

h) Accuracy of Information

We encourage all persons associated with River Region Early Education to let us know if they become aware of inaccuracies in the information we retain. We will respond promptly to any request for correction to data that is discovered to be inaccurate.

i) Maintaining Information

The Nominated Supervisor is responsible for keeping all service records required under the *Education and Care National Regulation*. Information will be updated regularly.

In keeping with the Early Childhood Australia (ECA) *Code of Ethics* (2008), the *Education and Care Services National Regulations* and the *Privacy Legislation*, educators and staff employed by the education and care service bound to respect the privacy rights of children enrolled and their families.

Every employee and the Approved Provider is required to sign a Confidentiality Statement

Confidential conversations that educators have with parents, or the supervisor has with educators will be conducted in a quiet area away from other children, parents, and educators. Such conversations are to be minuted and stored in a confidential folder.

j) Anonymity

Wherever appropriate we will give individuals the option of remaining anonymous when communicating with River Region Early Education, for example, in surveys.

6. Procedure

Nil

7. Sources

- Centre Support
- Information Privacy Principles www.privacy.gov.au/ publications/ipps.html
- Department of the Officer of the Privacy Commissioner - www.privacy.gov.au
- Early Childhood Australia - www.earlychildhoodaustralia. org.au
- Fair Work Australia

8. Relevant Legislation, Regulations and Standards

Legislation	
	Children (Education and Care Services National Law Application) Act
	Section 286 (2) of the Corporations Act 2001
	Privacy Act 1988 (Clth)
Education and Care Services National Regulation	
181	Confidentiality of records kept by approved provider
183	Storage of records & other documents
184	Storage of records after service approval transferred
Children (Education and Care Services) Supplementary Provision Regulation 2012	
75	Information and access to be denied to certain persons
96	Retention of records
98	Confidentiality guidelines
National Quality Standards	
1.3.3	Families are informed about the program and their child's progress.
4.2.2	Professional standards guide practice, interactions and relationships.
5.1.1	Responsive and meaningful interactions build trusting relationships which engage and support each child to feel secure, confident and included.
6.1.1	Families are supported from enrolment to be involved in the service and contribute to service decisions.

6.2.2	Effective partnerships support children's access, inclusion and participation in the program.
6.2.3	The service builds relationships and engages with its community.
7.1.2	Systems are in place to manage risk and enable the effective management and operation of a quality service.
Child Safe Standards	
3	Families and communities are informed and involved
4	Equity is upheld and diverse needs are taken into account
Early Years Learning Framework Learning Outcomes	
3	Children have a strong sense of wellbeing
Early Years Learning Framework Principles	
	Secure, respectful, and reciprocal relationships
Early Years Learning Framework Practices	
	Holistic, integrated, and interconnected approaches

9. Related Documents

Doc #	Attachments
NQS7.60 A1	Confidentiality Statement
NQS7.60 A2	Privacy and Confidentiality Statement
NQS7.60 A3	Archiving Procedure

Doc #	Intersections with other key documents
NQS7.56	Governance and Organisation Management Policy
NQS6.40	Enrolment and Orientation Policy
NQS4.30	Orientation of Employees and Students Policy
NQS7.61	Accessible Use of Electronic Media Policy

10. Document Control

Doc #	Doc Title	Version	Approved	Next Review
NQS7.60	Privacy and Confidentiality Policy	1	August 2016	August 2018
NQS7.60	Privacy and Confidentiality Policy	2	August 2019	August 2021
NQS7.60	Privacy and Confidentiality Policy	3	August 2021	August 2024
NQS7.60	Privacy and Confidentiality Policy (minor changes due to name change and new policy document format)	3a	January 2024	August 2024