



PRIVACY & CONFIDENTIALITY POLICY

The right to confidentiality and privacy of the child and the family is outlined in Early Childhood Code of Ethics and National Education and Care Regulations.

The right to privacy of all children, their families, educators and staff of Clarence Family Day Care Service will be upheld and respected, whilst ensuring that all children have access to high quality early years care and education.

PURPOSE

To ensure that the confidentiality of information and files relating to the children, families, staff, and visitors using Clarence Family Day Care is upheld at all times. We aim to protect the privacy and confidentiality by ensuring continuous review and improvement on our current systems, storage, and methods of disposal of records, ensuring that all records and information about individual children, families, educators, and management are held in a secure place and are only retrieved by or released to people who have a legal right to access this information.

SCOPE

This policy applies to all staff, committee members, educators and educator assistants of Clarence Family Day Care.

POLICY

Early Childhood Services are required to comply with Australian privacy law which includes the Privacy Act 1988 (the Act) which was amended in February 2017, with changes taking effect on 22 February 2018.

The new law introduces a Notifiable Data Breaches (NDB) scheme that requires Early Childhood Services, Family Day Care Services, and Out of School Hours Care Services to provide notice to the Office of the Australian Information Commissioner (formerly known as the Privacy Commissioner) and affected individuals of any data breaches that are "likely" to result in "serious harm."

Businesses that suspect an eligible data breach may have occurred, must undertake a reasonable and expeditious assessment to determine if the data breach is likely to result in serious harm to any individual affected. A failure to notify, that is found to constitute a serious interference with privacy under the Privacy Act, may result in a fine of up to \$360,000* for individuals or \$1.8 million* for organisations. *Note this amount can increase with indexation/CPI or when the Federal Government determines to increase the penalty amount.

In order to comply, services are required to follow the Australian Privacy Principles (APPs), which are contained in Schedule 1 of the Privacy Act 1988 (Privacy Act).

In particular, the principles cover how personal information can be used and disclosed (including overseas), keeping personal information secure, and the open and transparent management of personal information.

The principles cover:

- the open and transparent management of personal information, including having a privacy policy
- an individual having the option of transacting anonymously or using a pseudonym where practicable
- the collection of solicited personal information and receipt of unsolicited personal information including giving notice about collection
- how personal information can be used and disclosed (including overseas)
- maintaining the quality of personal information
- keeping personal information secure
- right for individuals to access and correct their personal information

The APPs place more stringent obligations on APP entities when they handle 'sensitive information'. Sensitive information is a type of personal information and includes information about an individual's:

- health (including predictive genetic information)
- racial or ethnic origin
- political opinions
- membership of a political association, professional or trade association or trade union
- religious beliefs or affiliations
- philosophical beliefs
- sexual orientation or practices
- criminal record
- biometric information that is to be used for certain purposes
- Biometric templates.

Australian Privacy Principles (APPs)

APP 1 – Open and transparent management of personal information

Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

APP 2 – Anonymity and Pseudonymity

Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

APP 3 – Collection of solicited personal information

Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information.

APP 4 – Dealing with unsolicited personal information

Outlines how APP entities must deal with unsolicited personal information.

APP 5 – Notification of the collection of personal information

Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

APP 6 – Use or disclosure of personal information

Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

APP 7 – Direct marketing

An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

APP 8 – Cross-order disclosure of personal information

Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

APP 9 – Adoption, use or disclosure of government related identifiers

Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier or use or disclose a government related identifier of an individual.

APP 10 – Quality of personal information

An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

APP 11 – Security of personal information

An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

APP 12 – Access to personal information

Outlines an APP entity's obligations when an individual request to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

APP 13 – Correction of personal information

Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.

The Approved Provider/Coordinators will:

- Provide Staff and Educators with relevant information regarding changes to law and Clarence FDC Service policy.
- Ensure all relevant staff understand the requirements under Australia's privacy law.
- Maintain currency with the Australian Privacy Principles (this may include delegating a staff member to oversee all privacy-related activities to ensure compliance).
- Ensure personal information is protected in accordance with our obligations under the Privacy Act 1988 and Privacy Amendments (Enhancing Privacy Protection) Act 2012.
- Ensure all records and documents are maintained and stored in accordance with Education and Care Service National Regulations.
- Ensure the FDC service acts in accordance with the requirements of the Privacy Principles and Privacy Act 1988 by developing, reviewing, and implementing procedures and practices that identify:
 - the name and contact details of the FDC service
 - what information the service collects and the source of information
 - why the information is collected
 - who will have access to the information
 - collection, storage, use, disclosure, and disposal of personal information collected by the service
- Comply with any law that requires the particular information to be collected.
- Provide adequate and appropriate storage for personal information collect by the service.
- Provide protection of personal information from unauthorised access.
- Ensure the appropriate and permitted use of images of children.
- Ensure all employees, students, volunteers, and families are provided with a copy of this policy.
- Deal with privacy complaints promptly and in a consistent manner, following the Clarence FDC Service's Grievance Procedures.
- Ensure families only have access to the files and records of their own children.
- Ensure information given to Educators will be treated with respect and in a professional and confidential manner.
- Ensure child and staff files are stored in a locked and secure cabinet.
- Ensure Information relating to staff employment will remain confidential and available only to the people directly involved with making personnel decisions.
- Ensure that information shared with us by the family will be treated as confidential unless told otherwise.

The Educator/Educator Assistants will:

- Adhere to FDC Service policies and procedures, supporting management.
- Not discuss personal information with other educators, their partners, children or anyone else who is not required to have the information.
- Ensure that no other household members and/or visitors can access records (hard

copies/electronic/online) related to FDC service including children records.

- Ensure volunteers and families are aware of the privacy and confidentiality policy.
- Ensure the FDC service obtains consent from parents and/or guardian of children who will be photographed or videoed by the service.
- Ensure documented information and photographs of children are kept secure but may be accessed at any time by the child's parents or guardian.
- Ensure families only have access to the files and records of their own children.
- Ensure that information shared with us by the family will be treated as confidential unless told otherwise.
- Ensure only necessary information regarding the children's day-to-day health and wellbeing is given to non-primary contact educators; for example, food allergy information.
- Ensure that information given to Educators will be treated with respect and in a confidential and professional manner.
- Not discuss individual children with people other than the family of that child, except for the purposes of curriculum planning or group management. Communication in other settings must be approved by the family beforehand.
- Treat private and confidential information with respect in a professional manner.

Personal information our FDC service may request in regard to children/families:

- Parent/Guardian contact details
- Emergency contact details and persons authorised to collect individual children
- Children's health requirements
- Immunisation records
- Developmental records and summaries
- External agency information
- Custodial arrangements
- Incident reports
- Medication reports
- Child Care Subsidy information
- Medical records
- Permission forms

Personal information our FDC service may request in regard to staff/educators/educator assistants/committee members:

- Personal contact details
- Tax information
- Working contract
- Emergency contact details
- Medical details
- Immunisation details
- Working with children check
- Insolvency Checks
- National Criminal History Record Checks
- Qualifications
- Medical history
- Resume
- Superannuation details
- Child Protection qualifications
- First Aid, Asthma and Anaphylaxis certificates

NATIONAL QUALITY FRAMEWORK

EDUCATION AND CARE SERVICES NATIONAL REGULATIONS	NATIONAL QUALITY AREA	NATIONAL QUALITY ELEMENT/STANDARD
168, 181 - 184	7	7.1 = 7.1.1, 7.1.2, 7.1.3 7.3

REFERENCE & RELATED INFORMATION

- Privacy Act 1988.
- Education and Care Services National Law
- Education and Care Services National Regulations
- Australian Childcare Alliance. (2019). Changes to Australia's privacy law: What ECEC services need to know: <https://childcarealliance.org.au/blog/115-changes-to-australia-s-privacy-law-what-ecec-services-need-to-know>
- Australian Children's Education & Care Quality Authority.
- Early Childhood Australia Code of Ethics. (2016).
- Guide to the Education and Care Services National Law and the Education and Care Services National Regulations.
- Guide to the National Quality Standard.
- Office of the Australian Information Commission – Australian Privacy Principles: <https://www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles>
- National Quality Standard.
- United Nations Convention of the Rights of a child.