NQS7 Governance and Leadership Policy
Privacy

Commitment

The Creche and Kindergarten Association Ltd (C&K) is committed to protecting the privacy of all people with whom we communicate. C&K will collect, hold, use and disclose only the personal information that is reasonably necessary to carry out our functions and activities, and will be bound by the Australian Privacy Principles set out in *the Privacy Act 1988* (Cth) (Privacy Act) and the *National Vocational Education and Training Regulator Act 2011* (Cth) (NVETR Act).

Australian Privacy Principles

We are committed to complying with the Australian Privacy Principles (APPs) as set out in the Privacy Act. This means we collect, use, and store your personal information in a way that is lawful, fair, and transparent. We only collect personal data that is necessary to achieve Our Purpose, and we ensure it is kept secure. We provide you with clear options to access, correct, or delete your personal information and take appropriate steps to protect it from unauthorised access or misuse. Additionally, we do not share or disclose your personal data to third parties without your explicit consent, except where required by law.

What personal information we may collect

C&K collects and uses 'personal information' (as defined in the Privacy Act) which is information or an opinion about an identified individual, or an individual who is reasonably identifiable which:

- may exist in any form, including verbal, written, or photographic
- applies regardless of whether the information is accurate or not
- may be recorded or not recorded
- includes details such as a person's name, address, contact information, social media platform username, date of birth and gender

Sensitive information (a subset of personal information) includes information about a person's:

- race or ethnic origin
- political opinions and memberships
- religious beliefs
- membership of a trade union or professional association
- sexual preferences or practices
- criminal record
- health information, including genetic, biometric, physical and mental health, disability, use of health services and vaccination status.

Why do we collect, hold, use and disclose your personal information

We collect, hold, use and disclose personal information to support our purpose of providing high-quality early childhood education and care, training educators, and supporting the broader sector. This includes using personal information to:

- **Deliver our services** – including education, care, training, curriculum delivery, and communication with you;
- **Operate and improve our organisation** – including administration, funding, research, program development, and service improvement;
- **Engage with our community** – including advocacy, marketing, and sharing information about children's engagement in educational activities (with appropriate consent);
- **Manage our workforce and partnerships** – including recruitment, student placements, and working with service providers;
- **Comply with legal and regulatory obligations** – including public health requirements, reporting, and disclosures required or authorised by law;
- **Manage risk and resolve issues** – including complaints, investigations, and safety and risk management.

We may also use and disclose personal information for purposes that are related to or reasonably necessary for these activities.

Australian Privacy Principles

The following sections explain how C&K complies with each Australian Privacy Principle (APPs) including our practices for handling, managing, and protecting your personal information.

APP1: Open and Transparent Management

We are committed to open and transparent management of your personal information. We take proactive steps to ensure that you are fully informed about how your data is collected, used, and protected. Our privacy practices are clearly outlined in this Privacy Policy, which provides detailed information on the types of personal information we collect, the purposes for which it is used, and how we safeguard it. We are transparent about our data processing activities and are committed to updating our privacy practices as necessary to reflect any changes in our services or applicable laws. Should you have any questions or concerns about how we handle your personal data, you are welcome to contact us for further clarification and assist you in understanding your privacy rights. Our Privacy Policy is publicly available and regularly reviewed.

APP2: Anonymity and pseudonymity

Wherever lawful and practicable, you may choose to interact with C&K anonymously or using a pseudonym (e.g. general website enquiries). However, for regulated services (enrolment, training, employment) we are legally required to identify individuals and cannot provide services anonymously.

APP3: How we collect your personal information

We collect only the personal information reasonably necessary to carry out our functions and activities and will not collect information unrelated to Our Purpose. The main way we collect information about you is when you give it to us. What information we collect and how we collect it is set out in the table attached to this Policy.

We will notify you when we are collecting your personal information. We will obtain your express consent to collecting sensitive information. If you don't want us to use your information you can tell us at the time it is collected or as soon as possible afterwards.

If you do not want C&K to collect and use your personal information, we may not be able to provide services to or assist you.

APP4: Unsolicited personal information

If C&K receives personal information that we did not request, we will promptly assess whether we need to retain it for our functions or activities. If not, we will destroy or de-identify it as soon as practicable, unless retention is required by law. We will only retain unsolicited information where it is reasonably necessary for our operations or to meet our legal or contractual obligations.

APP5: Notification of Collection

We provide collection notices at or before the time we collect personal information. Standard notices are available on our website and in enrolment forms. Our notices will include who is collecting the information, the purposes of collection, any consequences of not providing the information, and whether we disclose the information to any third parties.

APP6: How we disclose your personal information

We only use or share your personal information for the purposes described in this Privacy Policy, for which you have given consent, that you would reasonably expect, or as required or authorised by law. This may include sharing limited information with our service providers (e.g. Kidsoft CCMS, Storypark, Easy Employer, website analytics providers) under contracts that require privacy and security safeguards.

We will not use or disclose your personal information for other reasons unless:

- you have consented,
- it is directly related to the purpose for which your information was collected, and you would reasonably expect this use, or
- it is required or authorised by law.

A purpose is "directly related" if it is closely connected to, or necessary for, the services or functions for which your information was collected. For example, information collected for enrolment may also be used to communicate about your enrolment, issue statements or reports, or coordinate care and learning services.

APP7: Direct Marketing

We may use your personal information to tell you about our services, programs, or events that may interest you. You can opt out of receiving marketing communications at any time, and every message will include an easy way to unsubscribe. We will act on your request promptly. We will not use sensitive information for marketing without your consent, and we will not share your personal information with third parties for their marketing purposes without your consent.

APP8: Cross-Border Disclosure of Personal Information

Some of our service providers may store or process your personal information outside Australia. Before disclosing information overseas, we take reasonable steps to ensure it is protected in accordance with the *Privacy Act 1988* (Cth), including assessing whether the recipient is subject to a privacy regime with standards similar to Australia's, entering into contracts that impose appropriate privacy and security obligations, and, where required, obtaining your consent. We will only disclose information overseas for purposes consistent with this Privacy Policy or as otherwise required or authorised by law.

APP9: Government Identifiers

C&K does not adopt government-related identifiers as its own except as permitted by law.

APP10: Quality of Personal Information

We take reasonable steps to make sure the personal information we collect, use, or share is accurate, up-to-date, and complete. This includes checking information when it's collected, reviewing it regularly, and letting you update or correct your details. Keeping your information accurate helps us provide our services effectively.

APP11: How we store and protect your personal information

Most of the information we hold about you will be stored electronically. We take reasonable steps to protect your personal information as far as practicable by:

- storing information on secure servers or locations accessible only to persons authorised by C&K
- all employees regularly completing privacy training
- appropriately destroying personal information no longer required
- conducting internal assessments to determine privacy requirements and compliance with our security measures
- requiring our service providers to only use or disclose the information for the purpose of the service.

Unfortunately, no electronic system is guaranteed to be 100% secure. In the event of a data breach, we will take all necessary steps to contain and mitigate any risk and notify affected individuals and the Privacy Commissioner where required under the *Privacy Act 1988* (Cth).

APP12 & 13: How to access or correct your personal information

You have the right to access the personal information we hold about you and request corrections if you believe it is inaccurate, incomplete, or out-of-date. To do so, please contact our Privacy Officer at privacy@candk.asn.au. We may need to ask you to verify your identity before providing access or making corrections. We will respond to your request within 30 days, unless there is a lawful reason for delay. If we refuse a request for access or correction, we will provide reasons and, where appropriate, allow you to make a statement about the information which we will attach to your records.

Our privacy governance, practices and systems

C&K implements organisation-wide privacy practices, procedures and systems, including a Privacy Impact Assessment (PIA) process, a Data Breach Response Plan, mandatory privacy training, internal monitoring and reporting, and role-based accountability across governance bodies.

How to make a complaint

If you believe that C&K has breached your privacy, please contact C&K's Privacy Officer:

Email: privacy@candk.asn.au
Post: C&K Privacy Officer
257 Gympie Road
Kedron QLD 4031

The Privacy Officer will:

- acknowledge your complaint within five business days
- Investigate your complaint
- endeavour to respond to you with the outcome of the investigation within 30 business days.

If you make an anonymous complaint, we may not be able to properly investigate or respond to it.

When we review your complaint, we may need to contact the people you name and disclose to them your identity and the nature of your complaint. If you do not wish C&K to do so, please let us know. However, this may limit our ability to properly investigate and resolve your complaint.

If you are dissatisfied with C&K's response or believe your complaint remains unresolved, you may take your complaint to the Office of the Australian Information Commissioner. The contact details for the Office of the Australian Information Commissioner can be found via its website located at https://www.oaic.gov.au.

Amending this policy

We may change this policy at any time without prior notice. When we do make changes, we will notify you of them by posting an updated version of the policy on our website.

What personal information we collect and how we collect it

How we collect your personal information and the type of personal information that we collect about you and your family will vary, depending on how we interact with you. This includes, but is not limited to:

Enrolling your child at and attending a C&K branch centre

Information Collected	How it is collected
• Full name (of parents / guardian and child) • Address details (of parents / guardian and child) • Date of birth (of parents / guardian and child) • Gender • Relationship to child (of parent / guardian) • Contact details (phone number, email) • Your child's authorised health contacts, emergency contacts, persons nominated to collect your child from our centre • Copies of identification documents, such as your child's birth certificate or passport • Financial information such bank account and credit card detail (of enrolling parent / guardian) • Centrelink Customer Reference Number • Court orders, including custody arrangements • Booking and attendance records	C&K Website – online wait list application form Enrolment booklet – in writing and / or online (Kidsoft Childcare Management System)
• Photographs, video images, artwork or pictures (you can tell us if you do not wish us to use these for marketing purposes when you complete the enrolment booklet)	Children's portfolios (online through third party provider Storypark) Photographer
• Statistical information provided to the Department of Education	Online survey through third party provider
• Providing feedback to C&K	Website or in writing
Sensitive Information	
• Your child's nominated medical practitioner • Health information including Medicare number, details of a child's health care or dietary needs (including medical conditions and allergies and risk of anaphylaxis), medical management or risk minimization plan in relation to any medical conditions and immunisation status and records • Behavioural or developmental assessments • Religion, cultural background and language spoken at home • Any information relating to special requirements for a child's care (this may constitute sensitive information) • Vaccination status	C&K Website – online wait list application form Enrolment booklet – in writing and / or online (Kidsoft Childcare Management System)
• Biometric scanning information if you opt into using this functionality when you log into a centre using a biometric keypad	Online
• Health or medical information about your child's additional needs (for example when applying for additional needs funding)	In writing and / or online

If your child is waitlisted or enrolled at a C&K affiliate centre

Information Collected	How it is collected
• Full name (child) • Address details • Date of birth (child)	Affiliate Data Collection spreadsheet or Online via the Affiliate's Kidsoft Childcare Management System
• If you provide feedback to C&K	Website or in writing
Sensitive Information	
• Health information including details of a child's health care card, suspected or diagnosed disability • Religion, cultural background and language spoken at home • Any information relating to special requirements for a child's care (this may constitute sensitive information) • Health or medical information about your child's additional needs (for example when the affiliate centre is applying to C&K for inclusion support funding)	Affiliate Data Collection spreadsheet or Online via the Affiliate's Kidsoft Childcare Management System

Early Childhood Teachers (Affiliate Centres only)

Information Collected	How it is collected
• Name • Qualification and Qualification Status	Affiliate Data Collection spreadsheet or Online via the Affiliate's Kidsoft Childcare Management System

Students, Volunteers and External Contractors

Information Collected	How it is collected
• Name • Email Address • Contact Number • Blue card type • Blue card number • Blue card expiry date • Referee Name • Referee Position / Relationship • Referee Contact Details • Employment or Volunteer History • Health information (if required for safe participation) • Emergency Contact Name and Contact Details • Attendance records • Student, Volunteer /External Contractor Signature	In writing and / or online
• Identification document e.g. drivers' licence, passport • National Police Check (Criminal History) • Blue Card / Exemption Card (or similar) • University/college affiliation and course details • Qualifications and/or Certifications • AHPRA Registration	Photocopy or electronic / digital image

Student Practicum Placement

Information Collected	How it is collected
• Child's image • Learning agreements or contracts with the tertiary institution • Supervisor feedback or assessment notes • Insurance details	Electronic / digital image Trainer/assessor observation via Microsoft Teams if trainer/assessor unable to visit centre

Visitors

Information Collected	How it is collected
• Name • Date of Birth • Email Address • Contact Number • Blue card type • Blue card number • Blue card expiry date • Company Name • Position Title • Photographic Identification document e.g. drivers' licence (to verify identity) • Health information (if relevant for access or participation)	In writing and / or online / digital image

C&K Open Week Event (Families)

Information Collected	How it is collected
• Parent / guardian name • Child's name • Child's Date of Birth • Email Address • Postcode • Contact Number	In writing and / or online
• Photograph or video of you participating in the event	Electronic / digital Image

C&K Focus Group (external participants)

Information Collected	How it is collected
• Name • Postcode • Email address • Age • Whether you have children or nor • Ages of children • If you use a C&K service • Marital status • Gender	In writing and / or online

Attending a C&K Event

Information Collected	How it is collected
• Parent / guardian name • Child name • Address • Date of birth • Email address • Address • Contact Number	In writing and / or online
• Photograph or video of you participating in the event	Electronic / digital image

Visiting C&K's website and participating in C&K's social media

Information Collected	How it is collected
• Name (if provided) • Address (if provided) • Date of birth (if provided) • Email (if provided) • Contact number (if provided) • Social media handle • Details about your computer	www.candk.asn.au Facebook Twitter Instagram TikTok LinkedIn Cookies Web analytics
• Images	When you upload images to C&K's social media accounts such as Facebook

Web analytics and tracking

We use software such as (but not limited to) Google Analytics and Crazy Egg to collect data about your interaction with our website.

The sole purpose of collecting this data is to improve your experience when using our site.

Examples of the types of data we collect with these tools include:

- your device's IP address
- device screen size
- device type, operating system and browser information
- sessions
- page views
- conversions
- bounce rate
- session duration
- geographic location (city)
- referring domain and out link if applicable
- search terms and pages visited on our website
- date and time when pages were accessed on our website
- heat mapping to improve functionality

Cookies

Cookies are small data files transferred onto computers or devices by websites for record-keeping purposes and to enhance functionality on the website. Most browsers allow you to choose whether to accept cookies or not. If you do not wish to have cookies placed on your computer, please amend your browser preferences before accessing the C&K website.

Applying for employment with C&K/Employees

Information Collected	How it is collected
• Full Name • Address • Date of birth • Gender • Email • Contact number • Documents setting out your employment history (such as a resume or CV) • Qualifications • Identification Documents (e.g. drivers' licence) • Name and contact details of your personal referees • Working with Children Check (Blue Card/Exemption Card) • AHPRA Registration When you become a C&K employee: • Bank account details (for payroll) • Superannuation account details (for payroll)	In writing and / or online (Page Up)
Sensitive Information we may collect	
• Health information (disability, medical conditions affecting work) • National Police Check (Criminal History) • Religion, cultural background, and language spoken at home • Vaccination Status (if provided) • Tax File Number • Performance reviews or disciplinary records • Union membership	In writing and / or online (Page Up) Electronic / digital image

Providing a service to or entering into a contract or tender with C&K

Information Collected	How it is collected
• Name • Address • Email address • Contact Number • Financial information such as bank account details	In writing or via email Electronic / digital image

Hiring a C&K venue

Information Collected	How it is collected
• Name • Address • Email address • Contact Number • Financial information such as bank account or credit card details	In writing or via email

Entering a C&K premise that uses Closed Circuit Televisions for security monitoring

Information Collected	How it is collected
• Your image • Audio record of your voice	Closed Circuit Television recording

Enrolling and studying at the C&K College of Early Childhood

Information Collected	How it is collected
• Name • Address • Date of birth • Gender • Place of birth • Email • Contact numbers • Emergency contact names, contact numbers and relationship to you • Previous or current schooling • Employment status • Employment information including employer's name, your position and your supervisor's name • Learner Unique Identifier • Unique Student Identifier • Driver's Licence • Birth Certificate • Passport • Immicard • Citizenship Certificate • Certificate of Registration by Descent • Financial information such as tax file numbers, bank account and credit card details • FEE Help Status • Your signature • A parent/guardian's signature if you are under 18	Enrolment booklet – in writing
Sensitive Information	
• Religion, cultural background and language spoken at home • Medicare Card • Disabilities and assistance requirements	Enrolment booklet – in writing Electronic / digital image

Providing feedback or making a complaint to C&K

Information Collected (If provided)	How it is collected
• Name • Address • Email address • Contact Number • Details of your complaint which may include reference to personal or sensitive information that you provide to us	In writing or via website online form

Privacy Responsibilities Matrix

To ensure compliance with the ***Privacy Act 1988*** **(Cth)** and the **Australian Privacy Principles (APPs)**, it is essential that all employees understand their specific responsibilities in relation to the handling of personal information. The table below outlines the key roles and associated privacy responsibilities across all levels of C&K, helping to support a clear, accountable, and consistent approach to privacy management:

Role	Key Privacy Responsibilities
Board	• Provide strategic oversight of privacy risk • Approve the Privacy Management Framework • Review and monitor significant privacy issues or data breaches
Chief Executive Officer (CEO)	• Lead a culture of privacy compliance • Ensure resourcing and accountability for privacy across C&K • Report significant privacy issues or data breaches to the Board
Executive Management Group	• Embed privacy into operational and strategic planning • Oversee business unit compliance • Monitor risk and report significant issues to CEO and Privacy Officer
Privacy Officer	• Maintain the Privacy Policy and Data Breach Response Plan • Conduct and oversee Privacy Impact Assessments (PIAs) • Manage privacy complaints and data breaches • Coordinate C&K's response significant privacy issues or data breaches • Deliver privacy training and awareness programs • Report significant privacy issues or data breaches to the CEO
Legal, Risk and Governance Team	• Advise on legal obligations under the *Privacy Act 1988* (Cth) and other applicable laws • Review contracts and data sharing agreements for privacy compliance • Assist in breach response and regulatory reporting
Senior Leadership Team	• Implement privacy processes in their teams • Ensure employees are trained and follow internal data handling procedures • Identify and manage privacy risks • Report privacy risks and/or incidents to Privacy Officer • Support privacy investigations
Information Technology Manager and System Owners	• Maintain data security controls (e.g. access control, encryption, monitoring) • Assist in data breach detection and response • Implement systems that support APP compliance (e.g. data retention, audit logs) • Implement and maintain appropriate cybersecurity measures to protect personal information, including but not limited to firewalls, encryption, Single Sign-On (SSO), Multi-Factor Authentication (MFA), access controls, intrusion detection, and regular patching and system updates • Support secure data transfers and storage
All Employees, Students, Volunteers and Contractors (Working with Children)	• Handle personal information responsibly and only for authorised purposes • Complete mandatory privacy training • Immediately report suspected or actual breaches • Follow internal privacy and data protection procedures