NQS2 Health and Safety Procedure
eSafety

Background

C&K is committed to the safety and wellbeing of every child, including how they engage with digital technologies. While these technologies offer significant educational and developmental benefits, they also present a range of risks. Children may be exposed to harmful content, cyberbullying and emerging threats, including those introduced by Artificial Intelligence (AI). Managing children's digital safety (eSafety) requires ongoing vigilance and is a shared responsibility between children, families and the centre.

C&K's commitment to child protection and safeguarding aligns with Standard 8: Physical and Online Environments of the Queensland Child Safe Standards and recommended guidelines outlined in the ACECQA - Online Safety Guide and National eSafety Commissioner's eSafety Early Years Program.

This procedure is implemented alongside the definitions outlined in appendix one of this procedure.

Centre staff are NEVER permitted to:

- × Use, control or have on their possession a personal electronic device while working directly with children, unless prior authorisation has been obtained for an essential purpose, as outlined in *Safe Management of Personal Electronic Devices at Centres Procedure*.
- × Use or have on their possession a personal electronic storage device while working with children.
- × Permit a child to access and use their personal electronic device or online platform.
- × Allow a child unsupervised access and use of C&K-issued device for any length of time.
- × Share passwords of C&K-issued devices with children or non-authorised persons.
- × Allow children to access and use a new online game or content before assessing and determining suitability.

Responsibilities

Teachers and educators will:

- Use encrypted, password-protected C&K-issued electronic devices and C&K-approved online platforms. Restrict access to authorised centre staff only.
- Participate in professional development activities to strengthen knowledge of safe and appropriate engagement with digital technologies e.g. free online Digital Child modules. (Branch Centres Only) Complete mandatory online *IT Cyber Awareness* training module by the allocated due date.
- Only use C&K issued devices to capture, store and transmit images of children.
- Only capture, store and transmit images of children for the purposes of the education and care services program.
- Appropriately include eSafety concepts into the curriculum. Refer to trusted information i.e. eSafety Early Years Program for Educators, PlayingITSafe and Digital Child..
- Consider developing a *Centre Online Safety Agreement* in collaboration with children and families. Refer to the National eSafety Commissioner Website for guidance and resources to support this process.
- Share online safety information with families e.g. eSafety Commissioner Online Safety for Under 5s Booklet.
- Actively supervise and monitor children's use of digital technologies. Document strategies in centre-specific *Supervision Plan*. Determine the type of digital technology engagement appropriate for each situation.

1. **Guided activities:**
   - The child and teacher/educator are both actively engaged in the use of digital technology. The screen remains within the educator's line of sight. Educators narrate their actions and encourage discussion e.g. "I wonder what will happen when we…". This level of engagement must be used for all new or unfamiliar content.
2. **Supervised activities:**
   - The child controls the screen and participates in a familiar online activity, while the educator remains in the same room and engages with the child about their activity e.g. asking questions or making comments.
3. **Independent activities:**
   - The child engages in a familiar online activity independently. The educator is nearby (in the same room) and regularly checks in with the child to ask about what they are doing or watching. The child must be aware they can seek help if they encounter anything online that makes them feel uncomfortable, scared or upset.

- Proactively consult with Aboriginal and Torres Strait Islander families to understand their perspectives, concerns, and suggestions around children's digital technologies.
- Teach children to ask an adult's permission before engaging with new online content, game or downloading anything on either a personal or C&K-issued electronic device.
- Securely store C&K-issued devices outside hours of operation.

- Before introducing a new online game or content on a C&K-issued device, assess and determine suitability. Seek Early Childhood Pedagogy Advisor (Branch centres only) guidance and authorisation from the Centre Director/Nominated Supervisor or Responsible Person in Charge (RPIC):

  Assess suitability:
  - Fosters the values of friendship and respect.
  - Responds to children's current ideas, interests and learning.
  - Encourages creativity and exploration, rather than passive or repetitive actions.
  - Promotes diversity, inclusion and equity.
  - Is culturally, incorporating Aboriginal and Torres Strait Islander perspectives.

  Assess eSafety:
  - Use trusted eSafety providers endorsed by the eSafety Commissioner.
  - Use child friendly 'safe search' engines e.g. www.safesearchkids.com and www.kiddle.com
  - Never input or disclose children's personal information when using online game, app or networked toys.

- Use visual timers or agreed routines to manage children's screen time. Do not exceed National Government recommendations:
  - No screen time for children under 2 years.
  - No more than 1 hour per day for children aged 2 to 5 years.
  - No more than 2 hours per day of recreational screen time for school-aged children (this does not include screen time for schoolwork).

Incidents and reporting

Teachers and educators will:

- Be alert to potential signs of exposure to inappropriate material or online harm e.g. changes in behaviour, secrecy. Encourage children to talk to a trusted adult if they see or experience something online that makes them feel uncomfortable.
- Promptly escalate and report eSafety incidents to your Centre Director/Nominated Supervisor or RPIC, and when required, notify the regulatory authority, in accordance with *Child Centre Incident Reporting Procedure (Branch/Affiliate)*.

In addition to the reporting responsibilities outlined in the *Child Centre Incident Reporting Procedure (Branch/Affiliate),* online child sexual exploitation, like online grooming and extortion, can be reported to the Australian Centre to Counter Child Exploitation (ACCCE). The ACCCE, led by the Australian Federal Police, works with various agencies to prevent online child exploitation. Child sexual abuse material online should also be reported to the eSafety Commissioner. The Commissioner can take action to remove the content and other forms of harmful content.

Reporting suspected or actual breaches or misuse

Employees must report any use of C&K-issued (Branch Centres) or Affiliate-issued (Affiliate Centres) devices or digital technologies that may result in the accidental or intentional misuse, loss of, or unauthorised access to personal or sensitive information.

Employees will:

- Immediately report any accidental or intentional misuse, loss, or unauthorised disclosure of sensitive and personal information to C&K's Privacy Officer (Branch Centres) or Management Committee (Affiliate Centres) providing the following information.
  - Date and time of the alleged incident
  - Description of the alleged breach or concern
  - Names of individuals involved (if known)
  - Any devices, platforms, or systems used
  - Immediate actions taken to minimise the risk of serious harm (e.g. device secured, removed employee's access to device and/or digital technology).
- Preserve any evidence, including:
  - Devices or platforms involved (do not delete or alter content)
  - Screenshots or emails (if relevant)
  - Access logs or audit trails (if applicable).
- Do not attempt to investigate independently beyond initial reporting. Avoid deleting records or confronting employees without direction from C&K's Privacy Officer (Branch Centres) or Management Committee (Affiliate Centres).
- Cooperate with internal investigation procedures, including providing statements, attending meetings, and adhering to any confidentiality requirements.

- Notify families promptly (as directed by C&K's Privacy Officer (Branch Centres) or Management Committee (Affiliate Centres)) if their personal information was involved in a confirmed breach, including a clear explanation and any protective steps taken.
- C&K's Privacy Officer (Branch Centres) or Management Committee (Affiliate Centres) will determine if escalation to external authorities is required e.g. Queensland Police Service, Department of Education, Child Safety, and/or the Office of the Australian Information Commissioner.
- Respect confidentiality throughout the process, ensuring the identity of any children or staff involved is protected during investigations.

Centre Directors/Nominated Supervisors and Responsible Person in Charge will:

- Include this procedure as part of the induction process for all teachers and educators, including casual staff.
- Ensure C&K-issued electronic centre devices are password protected and consistently securely stored outside hours of operation.
- Ensure compliance with C&K Emergency phone procedure.
- Order/purchase electronic devices that are approved/endorsed by C&K/Affiliate Centre Executive Management Committee, in line with centre's budget and appropriate prior approval from management. Branch Centres: Use the online *ICT Equipment Request Form* to order or purchase electronic devices.
- Never purchase or use any type of online product or cloud-based platform not endorsed by C&K or Affiliated Centre Executive Management Committee OR portable electronic storage device.
- Periodically review and monitor centre compliance with this procedure, including the type and purpose of digital content accessed or used. Provide feedback promptly address any instances of non-compliance.
- Promptly seek IT team assistance (it@candk.asn.au) for any technical issue.

Early Childhood Education Managers/Affiliate Management Committees will:

- Include this procedure as part of the induction process for Centre Directors/Nominated Supervisors.
- Periodically review and monitor centre compliance with this procedure, including the type and purpose of digital content accessed or used. Provide feedback promptly address any instances of non-compliance.

C&K IT team and C&K IT Steering Committee/Affiliate Centre Executive Management Committee will:

- Maintain up-to-date knowledge of current best practices in eSafety, cyber security and digital privacy, and provide clear guidance to centres.
- Stay informed about emerging technologies and system updates to help prevent serious ICT issues regarding child safety, financial losses, cyber security threats, data leaks and privacy breaches.
- Minimise children's exposure to inappropriate online content by activating and regularly reviewing parental controls, filtering tools, and safe search settings on all C&K-issued electronic devices used by children.
- Ensure all C&K-issued devices are configured with appropriate privacy, eSafety, and cyber security protections. For example, Next-Gen Network Firewalls and Advanced Endpoint security.
- Regularly monitor the use of C&K-issued devices and approved online platforms to ensure they are used safely, appropriately, and in alignment with this and associated procedures.

Associated Policies and Procedure

This procedure is implemented alongside the following C&K policies and procedures:

- *Safe Use and Management of Children's Images Captured for Educational Programs Procedure*
- *Safe Management of Personal Electronic Devices at Centres Procedures*
- *Acceptable Use Procedure*
- *Acquisition and Provision of Hardware and Software Procedure*
- *Cyber Training Awareness Procedure*
- *Mobile Device Procedure*
- *Privacy Policy*
- *Supporting Relationships and Partnerships Procedure*
- *Artificial Intelligence (AI) Position Statement*

References and Resources

- eSafety Commissioner - *eSafety Early Years Booklet*
- Australian Federal Police/Alannah and Madeline Foundation – *Playing IT Safe*
- Allannah and Madeline Foundation - *eSmart*
- *ACECQA NQF Online Safety Guide*
- *Queensland Family and Child Commission Child Safe Standards*

Appendix one – Definitions

Images
Still photos and video recordings. Images of children are classified as personal information and are recorded, used and stored in strict compliance with the *Privacy Policy* and this procedure.

Electronic device
Any device capable of recording, storing, sharing or transmitting images, including but not limited to smartphones, wearable technology including smartwatches and smart glasses, tablets, cameras and computers.

Personal Electronic Device
Any electronic device owned or controlled by a person capable of capturing, storing or transmitting an image, that is not the property of C&K (as the Approved Provider) or Affiliated Centre Approved Provider. Examples include, but are not limited to, smartphones, tablets, cameras, computers, and wearable technology including smartwatches and smart glasses.

C&K-Issued Electronic Device
Any electronic device capable of capturing, storing or transmitting and image or storing or storing, sharing or transmitting images, that is the property of C&K (as the Approved Provider) or Affiliated Centre Approved Provider. Examples include, but are not limited to, to smartphones, tablets, cameras and computers.

Electronic Storage Device
USBs, portable hard drives and memory cards able to store and transport files and images.

C&K-Approved Online Platform
Any online or cloud-based platform/application endorsed by C&K (via the IT Steering Committee or Executive Management Committee) or Affiliated Centre Executive Management Committee. Storypark is the primary C&K-approved online platform used to document and share images of children for the purposes of the educational program.

Personal Online Platform
Any online or cloud-based platform not approved by C&K or the Affiliate Centre Management Committee, that can store, share or transmit images, that a C&K or affiliated centre employee, student, volunteer, or contractor who works with children has a registered account. Including but not limited to, personal email account, any type of social media account or web-based graphic design platform.

Working directly with children
Being physically present with a child or children at the time, and employed, engaged or appointed to provide education and care to the child or children at that time.