NQS2 Children's Health & Safety Procedure

Safe Use and Management of Children's Images Recorded for Educational Programs

Background

C&K is committed to protecting the safety and wellbeing of every child. This commitment extends to how images of children are recorded, used, shared and stored. This procedure aligns with the *National Model Code for Taking Images or Videos of Children while Providing Early Childhood Education and Care (National Model Code).*

This procedure outlines the safe, ethical and lawful use of children's images recorded for educational programs (internal use only). The images of children recorded for the purposes of marketing and social media (external use) are not in scope of this procedure.

Personal electronic devices are never used to record, share and store children's images

For the purposes of this procedure:

- **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 capable of recording, storing, sharing or transmitting images, that is the property of a C&K or Affiliated centre employee, student, volunteer or contractor that works with children. Examples include, but are not limited to, to smartphones, wearable technology including smartwatches and smart glasses, tablets, cameras and computers.
- **C&K-Issued Electronic Device:** A tablet or camera capable of recording, storing, sharing or transmitting images, that is the property of C&K or Affiliated Centre.
- **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.

Centre staff are NEVER permitted to:

- × Record, use, share, transmit, upload and store images of children:
  - without the prior written parent/guardian written consent.
  - for personal use.
  - on a personal electronic device, personal online product or portable electronic storage device.
  - on an electronic device or online product or cloud-based platform not approved by C&K/Management Committee.
- × Access any image of a child taken on a C&K-issued electronic device for personal use.
- × Install, access, purchase or use any type of online product or cloud-based platform on a C&K issued electronic device not endorsed by C&K/Management Committee.
- × Install or access a personal online platform on a C&K-issued electronic device.
- × Record images of children:
  - in bathrooms, toilets, nappy change room/areas, cot/infant sleep rooms, cubbies and any location where another centre staff member cannot see the image being taken.
  - not appropriately dressed, for example, in their underwear, in a state of undress, completely undressed or with their genitalia or underwear exposed.
  - in a position that could be perceived as sexualised in nature.
  - when injured or in an emotionally distressed state or dysregulation escalation.
- × Force or coerce a child to be in a photograph or video if they don't want to.
- × Compromise the active supervision of children or delivery of the program when recording images of children.
- × Store or transport images of children on portable hard drives or USBs.
- × Store images of children for more than 90 days on a C&K-issued electronic device.

Parent/Guardian Authorisation

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

- Upon receipt, review *Online Enrolment Form/Booklet* to check if parents/guardians have provided their consent for their child's image to be recorded and used for the educational program (internal use). Parent/guardian consent is recorded in childcare management system (Kidsoft).
- Respect and follow the direction of parent/guardians when they do not provide their consent for their child's image to be taken and used.
- Understand parent/guardian consent can be changed or withdrawn in writing (via *Use of Children's Images Permission Form*) at any time.
- Promptly inform teachers and educators and implement centre protocols to prevent a child's image to be recorded and shared, when parent/guardian consent has not been provided.

Recording and Using Children's Images

Teachers and educators will:

- When prior parent/guardian written consent has been provided, record and use images of children for purposes of the educational program, including but not limited to:
  - recording and assessing children's learning
  - Storypark documentation
  - printed portfolios
  - floor books
  - program documentation
  - social stories
  - project work
  - centre displays
  - internal professional development material
- Only use C&K-issued electronic devices and C&K-approved online platforms to record, edit, share and store images of children.
- In a developmentally appropriate way, seek a child's informed consent before capturing their image. Refer to the *ACECQA Information Sheet - Empowering children under 5 by asking them to give their consent* and EdHub article *From Happy Snaps to Safety: Reimagining Digital Documentation* for practical guidance.
- Teach children about their digital footprint i.e. how and why their image is used, stored and who can access.
- Prioritise quality over quantity. Avoid taking unnecessary images, superficial 'happy snaps' and storing an extensive number of images. Record and use images of children:
  - In a way that respects their rights, safety and security.
  - That positively showcases and documents their learning, including their strengths, interests and agency, and engagement with the learning environment and their peers.
  - That informs and supports pedagogical reflection and decision-making.
- Avoid or minimise disrupting children's learning and play when capturing images. Consider whether the moment would be better recorded through alternative documentation, such as a written observation. Consider: Is it more valuable to document this moment or to be present and emotionally responsive with the child?
- When appropriate, capture non-identifying images. For example, where a child's face is not visible, images focused on a child's hands, feet or the learning materials being used, and excluding identifying information such as name tags or recognisable backgrounds.

Storing and Archiving Children's Images

Teachers and educators will:

- Securely store children's images on encrypted, password-protected C&K-issued electronic devices and C&K-approved online platforms. Restrict access to authorised staff only. Do not share passwords with children or non-authorised persons.
- As per the steps outlined in appendix one of this procedure, confidentially delete children's images of children unintentionally captured, not used for the educational program or that do not meet the requirements outlined in the *'Recording and Using Children's Images'* section of this procedure.
- Within 90 days of an image's creation date:
  - Use image for the purposes of the educational program.
  - Where relevant, select images for historical record keeping and store securely on Centre's OneDrive.
  - Confidentially delete children's images of children as per the steps outlined in appendix one of this procedure.
- Store images of children on C&K-issued electronic devices for no more than 90 days. Complete a monthly audit via the *Safety Checklist*.
- Within 30 days of child's centre 'exit date', download child's Storypark portfolio ('archived child') and upload to child's Kidsoft record.

Reporting suspected or actual breaches or misuse

All employees have a duty of care to report any concerns regarding the inappropriate capture, storage or use of children's images. The following actions must be taken if a suspected or actual breach or misuse of images occurs.

Teachers and educators will:

- Immediately report any accidental or intentional misuse, loss or unauthorised disclosure of children's images to C&K's Privacy Officer (Branch Centres)/Management Committee including the following information.
    - Date and time of the incident
    - Description of the breach or concern
    - Names of individuals involved (if known)
    - Any devices, platforms, or systems used
    - Actions taken at the time (e.g. device secured)
- 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 images or confronting employees without direction from C&K's Privacy Officer (Branch Centres)/Management Committee.
- 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)/Management Committee) if their child's image was involved in a confirmed breach, including a clear explanation and any protective steps taken.
- C&K's Privacy Officer (Branch Centres)/Management Committee 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.

Management Responsibilities

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.
- Order/purchase electronic devices endorsed by C&K/Management Committee in accordance with centre budget and appropriate prior approval. Branch centre Directors order/purchase electronic devices via the online *ICT Equipment Request Form*.
- Periodically review and monitor centre compliance with this procedure, including what and how images of children are recorded and used. Provide feedback and promptly address and action non-compliance.
- Treat any use of personal electronic devices, personal online platforms or electronic storage devices that is inconsistent with this procedure as serious misconduct.
- Immediately report procedural non-compliance to the ECEM/Management Committee and, if required and where there is risk to children's health and safety, notify the regulatory authority in line with the *Child Centre Incident Reporting Procedure* (Branch/Affiliate).
- Ensure C&K-issued electronic devices are password-protected and consistently securely stored outside hours of operation.
- 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 what images are captured and used. Provide feedback and promptly address and action non-compliance.
- Treat any use of personal electronic devices, personal online platforms or electronic storage devices that is inconsistent with this procedure as serious misconduct

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

- Maintain a current register of C&K-issued electronic devices and C&K-approved online platforms.
- Maintain knowledge of current best practices in eSafety, cyber security and digital privacy, and provide clear guidance to centres.
- 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.
- Promptly and appropriately address any technology-related or online safety concerns, ensuring that timely and corrective action is taken to ensure children's images remain secure and confidential, and children's safety is always prioritised.
- Ensure all C&K-issued electronic devices and C&K-approved online platforms that capture, store and share children's images are password-protected, and where required, enable multifactor authentication.
- Conduct thorough due diligence before endorsing any online product or cloud-based platform for centre use. Refer to best practice safety guidelines from appropriate authorities before making decisions related to software and hardware e.g. eSafety Commissioner.
- Regularly monitor the use of C&K-issued devices and C&K-approved online platforms to ensure they are used safely, appropriately, and in alignment with this and associated policies and procedures.

Associated policies and procedures

This procedure is implemented alongside the following policies and procedures:

- *Safe Management of Personal Electronic Devices at Centres Procedure*
- *Privacy Policy (branch centres only)*
- *StoryPark Procedure*
- *Planning and Documenting Children's Learning and Teaching Practices Procedure*
- *Centre Based Student Procedure and Induction Checklist (branch centres only)*
- *Volunteers Working with Children and Induction Checklist (branch centres only)*
- *External Contractors Working with Children and Induction Checklist (branch centres only)*
- *Information Security Policy (branch centres only)*
- *Acceptable Use Procedure (branch centres only)*
- *Acquisition and Provision of Hardware and Software Procedure (branch centres only)*
- *Mobile Device Procedure (branch centres only)*
- *Artificial Intelligence (AI) Position Statement*

References and resources

- *National Model Code for Taking Images or Videos of Children while Providing Early Childhood Education and Care (National Model Code)*
- *ACECQA Child Safety – NQF Online Safety Guide*
- *ACECQA Information Sheet - NQF Child Safety Changes*
- Digital Child – *Resources for educators*
- Edhub - *From Happy Snaps to Safety: Reimagining Digital Documentation*

Appendix One - Confidentially Deleting Images

Windows Computer

1. **Open File Explorer:**
   Press Windows + E on your keyboard.

2. **Navigate to the folder** where the images are stored (e.g., Pictures, Downloads, Desktop, etc.)

3. **Select the images you want to delete:**
   Click once on an image to select it.
   Hold Ctrl and click multiple images to select more than one **or**
   press Ctrl + A to select all files in the folder.

4. **Delete:**
   Press the Delete key on your keyboard, **or**
   Right-click the selected image(s) and click Delete.

5. **Confirm deletion** (if prompted).
   The files will go to the Recycle Bin.

6. **To permanently delete them:**
   Right-click on the Recycle Bin and choose Empty Recycle Bin.

Apple iPad

Deleting Individual Photos	1. **Open Photos:** Launch the Photos app on your iPad. 2. **Select Photo(s):** Tap "Select" (or swipe down to see the photo grid and then tap "Select") and then tap on the photos you want to delete. 3. **Delete:** Tap the trash can icon. 4. **Confirm:** Tap "Delete Photo" (or "Delete [Number] Photos/Videos") to confirm. 5. **Recently Deleted:** The photos are now in the "Recently Deleted" album. You can recover them within 30 days or choose to permanently delete them.
Deleting Multiple Photos	1. **Open Photos:** Launch the Photos app. 2. **Select Photos:** Tap "Select", then tap on the photos you want to delete or swipe across multiple photos to select them efficiently. 3. **Delete:** Tap the trash can icon. **Confirm:** Tap "Delete Photo" (or "Delete [Number] Photos/Videos").
Permanently Deleting Photos from Recently Deleted: (Will happen automatically after 30 days)	1. **Open Photos:** Launch the Photos app. 2. **Go to Recently Deleted:** Tap "Recently Deleted" under Utilities. 3. **Select Photos:** Tap "Select", then tap the photos you want to permanently delete, or tap "Select All". 4. **Delete:** Tap "Delete" (or "Delete All"). 5. **Confirm:** Tap "Delete" (or "Delete All") again to confirm