NQS2 Health and Safety Procedure
Children's eSafety (Branch centres only)

C&K Commitment

The National Principles for Child Safe Organisations recognise the importance of safe online environments to promote the safety and wellbeing of all children. C&K is committed to protecting children's safety and wellbeing when engaging with online technology as part of our program delivery. C&K acknowledge that including access to online technology has many benefits for young children, including opportunities to be creative, practise language skills, solve problems, think critically, and develop relationships.

C&K teachers and educators play an important role in supporting children's learning and development in relation to technology and online safety. Through active engagement, explicit teaching and close supervision children should:

- Understand that the Internet is a connected network and there are benefits and risk when online.
- Be able to identify respectful behaviours both online and offline.
- Be able to identify and seek help from trusted adults in relation to negative online experiences.
- Be able to share how technology helps children and their family.
- Be able to inquire and ask questions about the things they see, say and do when online.
- Be able to give and ask for consent in relation to digital images and information.
- Be able to identify that there are safe and potentially unsafe interactions that can occur online.

(Playing IT Safe 2020)

eSafety Commissioner

This procedure reflects current safety strategies outlined in the eSafety Early Years Program developed by the National eSafety Commissioner and will be implemented alongside the following C&K policies and procedures:

- *IT Acceptable Use Policy*
- *IT Cyber Security Policy*
- *Mobile Devices Policy*
- *Online Learning Procedure*
- *Use of Multimedia and Information Technology for Learning and Teaching Procedure*
- *Privacy Policy*

Responsibilities

Managing children's eSafety is a shared responsibility.

C&K

- Minimise children's exposure to inappropriate content by activating online controls and safe search settings on all online devices used by children.
- C&K implements multiple cyber security measures to ensure online safety for the children, families, and staff. These measures include but not limited to Next-Gen Network Firewalls with web and content filters enabled as well as Advanced Endpoint security on all devices owned by C&K.
- Seek written consent from parents/guardians via the Enrolment Booklet/Consent Forms to collect, store, use and manage children's images, videos and audio recordings for the purposes of the educational program, and marketing and social media in accordance with the Privacy Policy.
- The Information Technology Team will provide a secure corporate network and advice on eSafety and cyber security best practices.
- The Legal Risk and Governance Team will provide advice on risk and privacy considerations.

Teachers and Educators

- Whenever children are engaged in online activities they must be closely supervised. Your centre's Supervision Plan must include supervision strategies when children are engaged in online activities.
- Determine which online activities will be:

Guided activities	Supervised activities	Independent activities
Child and teacher/educator are both engaged in an online activity and the screen remains within your sight. All new apps, games and content must be guided activities. Describe what you are thinking or doing and ask questions e.g., 'I wonder what will happen when we….'	Child has control of the screen and engages in a familiar online activity with a teacher/educator who is close by, talking with them about the online activity.	Child engages in a familiar online activity by themselves. Teacher/educator is close by, regularly 'checking in' with the child, asking them what they are doing or watching. Child is aware they can seek teacher/educator support if they see or experience anything online that makes them feel uncomfortable, scared, or upset.

- Consistently use password, fingerprint, or face recognition protection on all online devices.
- Consider developing a centre online safety agreement in collaboration with children and families. Refer to the National eSafety Commissioner Website for resources and information to support your centre through this process.
- Use child friendly 'safe search' engines e.g., Google Safe Search (www.safesearchkids.com) and Kiddle (www.kiddle.co).
- Escalate any eSafety incidents or concerns to your ECEM/C or IT team when appropriate in accordance with C&K policies and procedures.
- Share eSafety information with families (when appropriate).g. https://www.esafety.gov.au/parents, https://playingitsafe.org.au/parents-and-carers/

Incorporating eSafety concepts into the curriculum

Teachers and educators will:

- Teach children to ask an adult/teacher/educator permission before engaging with a new program, game, website or downloading anything onto a device.
- Refer to the eSafety Early Years Program (National eSafety Commissioner) and the Playing IT safe Website for curriculum ideas and resources.
- Appropriately incorporate child friendly online content and activities that are integral to the curriculum and support children's learning and development. E.g.,
  - Fosters values of friendship and respect.
  - Provides opportunities for learning.
  - Encourages creativity and exploration, rather than repetitive actions.
  - Promotes diversity and equity. For example: ABC Kids (abc.net.au/abckids), CBeebies (cbeebies.com) and PBS Kids (pbskids.org).
- Facilitate discussions with children to build their understanding of how people and technologies connect (or 'talk') to one another. Help children identify 'safe people' online, i.e., family, and close friends.
- In collaboration with families, support children's understanding of what is 'personal information' e.g., their name, date of birth, address, contact information and photos that identify them, and what information and images are OK to share and what needs to be kept private.
- Seek children's consent before sharing and posting their image, recordings, and information about them online. As often as you can, ask children if they would like to be in a photo before you take it. Ask before you share a photo, video, or write something about them on online (e.g., Storypark). Let them know who will see it and why you want to share it. Respect their decision if they do not want to share.
- Show children how to be kind and respectful online and model good habits around device use and online sharing, e.g.,
  - With toddlers and preschoolers explain that being kind online helps to ensure everyone has a good time.
  - Talk to preschoolers about the risks of cyberbullying as they get older and help them to identify who to ask for help if someone is unkind to them online.
- Support children to think critically about online content by facilitating discussion and seeking their ideas.
- Involve children in deciding on the right amount of screen time. Timers may be used to manage the amount of time children are online. Refer to the National Physical Activity and Sedentary Behaviour, and Sleep Recommendations for Children (Birth to 5 years) for sedentary behaviour recommendations.

Parents/Guardians

- Promptly raise any questions or concerns relating to their child's use of technology at home or at the centre with their child's educator.

References

- eSafety Commissioner - *eSafety Early Years Booklet*
- Australian Federal Police/Alannah and Madeline Foundation – *Play IT Safe*