CYBER SAFETY POLICY

Cyber safety is the safe and responsible use of Information and Communication Technologies (ICT). It involves being respectful of other people online, using good 'netiquette' (internet etiquette), and above all, is about keeping information safe and secure to protect the privacy of individuals. Our Service is committed to create and maintain a safe online environment with support and collaboration with staff, families and community.

NATIONAL QUALITY STANDARD (NQS)

QUALITY AREA 2: CHILDREN'S HEALTH AND SAFETY		
2.2	Safety	Each child is protected
2.2.1	Supervision	At all times, reasonable precautions and adequate supervision ensure children are protected from harm and hazard.
2.2.2	Incident and emergency management	Plans to effectively manage incidents and emergencies are developed in consultation with relevant authorities, practiced and implemented.
2.2.3	Child Protection	Management, educators and staff are aware of their roles and responsibilities to identify and respond to every child at risk of abuse or neglect.

EDUCATION AND CARE SERVICES NATIONAL REGULATIONS	
168	Education and care services must have policies and procedures
181	Confidentiality of records kept by approved provider
195	Application of Commonwealth Privacy Act 1988
196	Modifications relating to National Education and Care Services Privacy Commissioner and Staff

RELATED POLICIES

Code of Conduct Policy Technology Usage Policy Programming Policy Photography Policy	Family Communication Policy Privacy and Confidentiality Policy Record Keeping and Retention Policy

PURPOSE

To create and maintain a cyber safe culture that works in conjunction with our Service philosophy, and privacy and legislative requirements to ensure the safety of enrolled children, educators and families.

SCOPE

This policy applies to children, families, staff, management, and visitors of the Service.

TERMINOLOGY	
ICT	Information and Communication Technologies
Cyber safety	Safe and Responsible use of the internet and equipment/devices, including mobile phones and devices.
Netiquette	The correct or socially acceptable way of using the internet.

IMPLEMENTATION

Cyber Safety encompasses the protection of users of technologies that access the Internet, and is relevant to devices including computers, iPads and tablet computers, mobile and smart phones and any other wireless technology (including personal wearable devices- smart watches). With increasingly sophisticated and affordable communication technologies, there is a candid need for children and young people to be informed of both the benefits and risks of using such technologies. More importantly, safeguards should be in place to protect young children from accidentally stumbling upon or being exposed to unsuitable material or content.

Our Service has demanding cyber safety practices and education programs in place, which are inclusive of appropriate use agreements for Educators and families. Our educational software program provides families with up to date information about their child's development in way of daily reports, observations, photos, portfolios and email communications.

The cyber safety agreement includes information about the software program, the Services' obligations and responsibilities, and the nature of possible risks associated with internet use, including privacy and bullying breaches. Upon signing the Service's agreement, families and educators will have access to the educational software program.

Educational Software Program

Our Service uses OWNA which is a password protected private program for children, educators and families to share observations, photos, videos, daily reports, and portfolios. Families are able to view their child/children's learning and development and contribute general comments relating to their child or comment on an observation or daily report.

Educators are alerted via OWNA notification and on their dashboard when a family member has added a comment. Likewise, families are notified when a relevant educator has posted a photo/comment about their child.

Access to a child's information and development is only granted to a child's primary guardians. No personal information is shared with any third party.

OWNA is a private, secure online platform and dedicated mobile app using the latest SSL technologies that makes sharing key moments between educators and families more engaging. Real time updates for child/ren so parents know when their child(ren) has eaten, slept, had a nappy changed or even how much milk/water they've consumed. This is a reciprocal communication tool for educators/parents to use, sharing child/ren's learning with comments, photos & videos and keep up to date with Centre activities/events.

Confidentiality and privacy:

- The principles of confidentiality and privacy extend to accessing or viewing and disclosing information about personnel, children and/or their families, which is stored on the Service's network or any device.
- Privacy laws are such that educators or other employees should seek advice from Service management regarding matters such as the collection and/or display/publication of images (such as personal images of children or adults), as well as text (such as children's personal writing)
- A permission to publish form must be signed by parents to ensure children's privacy, safety and copyright associated with the online publication of children's personal details or work.
- All material submitted for publication on the Service Internet/Intranet site should be appropriate to the Service's learning environment.
- Material can be posted only by those given the authority to do so by the Service management.
- The Service management should be consulted regarding links to appropriate websites being placed on the Service's Internet/Intranet (or browser homepages) to provide quick access to sites.

child care
CENTRE DESKTOP

MANAGEMENT WILL ENSURE:

- All staff, families and visitors are aware of the Service's Code of Conduct and Confidentiality and Privacy Policies.

- The Service works with an ICT security specialist to ensure the latest security systems are in place to ensure best practice. Anti-virus and internet security systems including firewalls can block access to unsuitable web sites, newsgroups and chat rooms. However, none of these tools are fool proof; they cannot be a substitute for active adult supervision and involvement in a child's use of the internet.

- Backups of important and confidential data is made regularly (monthly is recommended)

- Backups are stored securely either offline, or online (using a cloud-based service)

- Software and devices are updated regularly to avoid any breach of confidential information

NOMINATED SUPERVISOR/ RESPONSIBLE PERSON / EDUCATORS WILL:

- Ensure to use appropriate netiquette and stay safe online by adhering to Service policies and procedures.

- Keep passwords confidential and not share with anyone.

- Log out of sites to ensure security of information

- Never request a family member's password or personal details via email, text, or Messenger.

- Report anyone who is acting suspiciously or requesting information that does not seem legitimate or makes you feel uncomfortable (See 'Resources' section for where to report).

- Permission for children to use computers is obtained by parents as part of the enrolment procedure.

- Ensure that children are never left unattended whilst a computer or mobile device is connected to the internet.

- Personal mobile phones are not used to take photographs, video or audio recordings of children at the Service.

- Only use educational software programs and apps that have been thoroughly examined for appropriate content prior to allowing their use by children.

- Provide parents and families with information about the apps or software programs accessed by children at the Service.

- Ensure that appropriate websites are sourced for use with children **prior** to searching in the presence of children.

- Use a search engine such as 'Kiddle' rather than Google to search for images or information with children (See 'Resources' section).

- Notify the Office of the Australian Information Commissioner (OAIC) by using the online Notifiable Data Breach Form in the event of a possible data breach. This could include:

child care
CENTRE DESKTOP

- A device containing personal information about children and/or families is lost or stolen (parent names and phone numbers; dates of birth, allergies, parent phone numbers).

- A data base with personal information about children and/or families is hacked

- Personal information about a child is mistakenly given to the wrong person (portfolios, child developmental report)

- This applies to any possible breach within the Service or if the device is left behind whilst on an excursion

FAMILIES

- When sharing anything using technologies such as computers, mobile devices, email, or any device that connects to the internet it is important you and everyone else invited to your account understands about netiquette and staying safe online and ensures privacy laws are adhered to.

- When it comes to your own children, it is your choice what you share outside of the Service. Remember though that young children cannot make their own decisions about what gets published online so you have a responsibility to ensure that whatever is shared is in your children's best interests.

- Be mindful of what you publish on social media about your child as this may form part of their lasting digital footprint.

- Install Family Friendly Filters to limit access to certain types of content on devices such as mobile phones and computers.

- Install parental controls on streaming services to ensure children are not able to access inappropriate material.

- Consider developing a *Family Tech Agreement* to establish rules about use of devices at home.

- Sometimes other children in the Service may feature in the same photos, videos, and/or observations as your children. In these cases, never duplicate or upload them to the internet/social networking sites or share them with anyone other than family members without those children's parents' permission.

- Access further information about eSafety to help protect your children and be cyber safe.

child care
CENTRE DESKTOP

RESOURCES

Australian Government Office of the eSafety commission www.esafety.gov.au/early-years

eSafety Early Years Online safety for under 5s. https://www.esafety.gov.au/sites/default/files/2020-02/Early-years-booklet.pdf

eSmart Alannah & madeline foundation www.esmart.org.au

Family Tech Agreement. eSafety Early Years Online safety for under 5s
https://www.esafety.gov.au/sites/default/files/2020-01/Our%20Family%20Tech%20Agreement_0.pdf

Kiddle is a child-friendly search engine for children that filters information and websites with deceptive or explicit content: https://www.kiddle.co/

Receive information on scams that can then be provided to the public. To report an online scam or suspected scam, use the form found here: https://www.scamwatch.gov.au/report-a-scam

 More information on online fraud and scams can be found on the Australian Federal Police website: https://www.afp.gov.au/what-we-do/crime-types/cyber-crime/online-fraud-and-scams

Notifiable Data Breaches scheme (NDB) can be made through the Australian Government Office of the Australian Information Commissioner

SOURCE

Australian Children's Education & Care Quality Authority. (2014).

Australian Government eSafety Commission (2020) www.esafety.gov.au

Australian Government Office of the Australian Information Commissioner (2019) https://www.oaic.gov.au/privacy/notifiable-data-breaches/about-the-notifiable-data-breaches-scheme/

Early Childhood Australia Code of Ethics. (2016).

Guide to the Education and Care Services National Law and the Education and Care Services National Regulations. (2017).

Guide to the National Quality Standard. (2020)

Privacy Act 1988.

Revised National Quality Standard. (2018).

REVIEW

POLICY REVIEWED	MARCH 2020	NEXT REVIEW DATE	MARCH 2021
MODIFICATIONS	• Additional content added • Additional information added to Family section • Resources added		
POLICY REVIEWED	PREVIOUS MODIFICATIONS		NEXT REVIEW DATE
OCTOBER 2019	• Notifiable Data Breach Scheme information added • Re-worded introduction • Resources section added • Additional information added to points • Sources checked for currency • Sources alphabetised		MARCH 2020
MARCH 2018	• Updated to comply with changes to the Australian Privacy Act		MARCH 2019
NOVEMBER 2017	• Updated Policy to comply with the revised National Quality Standard		MARCH 2018
MARCH 2017	• Reviewed policy, no changes made.		MARCH 2018

child care
CENTRE DESKTOP