Cyber Safety

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.

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

Technology Usage 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. 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 StoryPark 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 email and on their dashboard when a family member has added a comment. Likewise, families are notified via email when a relevant educator has posted 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.

With our use of the StoryPark app, parents will be in-the-know about their child's learning journey. When we document a child's experiences, parents are notified and able to view them right away.
All families at OLS have access to StoryPark. Parents are the administrators of their child's account and you are able to invite family and friends anywhere in the world (if you wish) to follow, comment and engage in your child's learning – perfect for families and friends who live overseas.

1   **What we post on Storypark:**
   o   **Learning stories:** Photos, videos and audio of your child's learning and play experiences
   o   **Group stories:** Images and videos of your child's interaction with other children and educators
   o   **Special moments:** Key moments in your child's development or fun activities like drawing or gardening
   o   **Event reminders:** Notices about important events at the centre, such as educational sessions

2   **Storypark Features**
The Storypark program gives you and your family an easy avenue for staying connected and excited about your child's learning journey.

As a user-friendly application, Storypark offers:
   o   A secure electronic sign-in/sign-out system
   o   Parental control of their child's portfolio
   o   Easy conversation and commenting tools
   o   Quick visibility of a child's learning progression
   o   Information about learning frameworks
   o   Option to invite specialists or aides to your child's portfolio

o   Compatability with iOS and Android

Storypark enhances parental and family involvement in your child's learning, because everyone stays up-to-date. The Storypark ePortfolio can be accessed and utilised from birth to school.

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)
- Ministry of Education guidelines are followed regarding issues of 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.

Management will ensure:

- The Service works with an ICT security specialist to ensure the latest security systems are in place to ensure best practice. Such systems and 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.

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.
- 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).

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

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

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

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.

- 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.

Resources

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

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

Source

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

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. (2017).

Privacy Act 1988.

Revised National Quality Standard. (2018).

REVIEW

POLICY REVIEWED	March 2019	NEXT REVIEW DATE	March 2020
MODIFICATIONS	Re-worded introduction. Resources section added. Additional information added to points Sources checked for currency. Sources alphabetised.		
POLICY REVIEWED	PREVIOUS MODIFICATIONS		NEXT REVIEW DATE
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