2.12 Safe Online Environments for Children/Young People

Policy Statement

This policy outlines OSHC's commitment to protect children and their welfare in online environments. As a service, we recognise the increasing use of digital platforms for learning and communication and develop practices that create security in an online environment, where children—

- Are guarded from harm and exploitation.
- Have their reputation, data and privacy protected.
- Are not exposed to inappropriate content.

Guided by the Best Practice Framework for Online Safety Education and eSafety Early Years program for educators published by the eSafety Commissioner. The service's policy aims to balance the dignity and affordance of using digital devices, and in a manner that still safeguards child's wellbeing and interests. The service's procedures will continue to be assessed and improved. We aim to continue collaboration with children (and families) to empower their participation around the design and development of our protocols for safely using devices at OSHC.

This policy applies to all children/young people, staff, volunteers, and parents connected to OSHC and covers all online activities, digital communications, and use of online learning platforms. The nature of technology means there are many opportunities for online environments to intersect with the service cross at several junctures and stakeholders including—

- Access to technology and the internet at OSHC.
- Taking photos and videos.
- Social media use by the community, including educators.

The service's policy sets out clear and explicit expectations for the community to use and interact online in a manner that maintains the safety and wellbeing of children. Anyone acting in a manner incompatible with our commitment to the safety and wellbeing of children may be exposed to disciplinary action relevant to the circumstance.

Key Tasks and Responsibilities

Managing Infrastructure	The Approved Provider is responsible for ensuring the service has suitable protections established, where children may access the internet as part of the program. The Nominated Supervisor or Responsible Person is responsible for ensuring the safeguards are working as intended.
Providing Supervision	All educators, especially those tasked with leading specific activities, are responsible for supervising children using devices and accessing content.

Professional Communication Interactions	All educators are expected to behave in the manner set out in policy to ensure children's safety and wellbeing is not compromised. Any concerns are brought to the attention of the Nominated Supervisor to address.

Procedures

Infrastructure and Technology

Children/Young People

1. Any children using devices – connected to the internet or not - must be properly supervised in an open environment. Educators must be able to easily view screens at any moment.
2. Any access to the internet must be approved and is only made available when filtering and/or monitoring systems are enabled.
3. In upholding our commitment to health and physical activity, access to devices (i.e. screen-time) will be limited -
    a. BSC, ASC and Vacation Care sessions - some restricted leisure time is made available with times set out in the program.
4. Where devices and media are made available these are to only contain content that is appropriate for children, using government classifications (G and PG-rated) as the guiding principle.
5. Children are not to take photos or videos of other children on their personal devices.

Educators

1. Sufficient and suitable equipment is available for educators to complete relevant tasks, such as programming and documentation.
2. Educators are not to use personal devices for any documents or material that may contain the personal information of children and families, this includes—
    a. Taking pictures on phones.
    b. Writing observation on personal devices.
    c. Emailing/messaging parents from personal accounts.
3. To remove any doubt, personal devices may be used for work activities that do not store or save children and families personal information, for example—
    a. Attending a webinar.
    b. Researching programming ideas.
    c. Communicating staffing arrangements.
4. Where an educator believes additional equipment is needed, they should communicate this to the Nominated Supervisor.

Communication and Information Sharing with Families

Child Care Software

The service upholds requirements for privacy and data by using reputable child care software to collect and store the substance of family's personal and sensitive information (i.e. enrolment information). This system is password protected and allows parents to more easily access the information retained by the service.

Email (or other Messaging)

At times, communication with families will occur via email. Where the service's representatives use email to communicate, must only occur on accounts owned and managed by the service.

Social Media

The service avoids publishing any personal or identifiable information (including photos and video) on its social media accounts (regardless of privacy settings). Any personal information is only posted in limited exceptions, and where authorisation has been provided in writing.

Where an educator becomes aware of a child being impacted or a risk of harm from an online setting (i.e. disclosure of cyber-bullying), then the service will inform the parent of this information at the earliest convenience.

Employee Social Media and Online Communication

Responsibility

All employees have a duty to uphold the reputation and interests of the service beyond the hours they are at work (see Code of Conduct). Educators have a responsibility to ensure their conduct is compatible with their employment obligations when using social media for personal use.

Communication and information sharing via social media or otherwise has the potential to harm either a child/family or the service's reputation. Any instances of a child or their family's privacy, reputation or safety being compromised will be treated very seriously. Employees engaging in this conduct will be subject to disciplinary action, up to and including termination.

Boundaries for Online Communication and Interactions

- There should not be any personal interaction with children of the service via social media, including being 'friends' or following accounts etc. If a child of the service attempts to interact with an educator, they should—
    - not respond,
    - review their privacy settings, and
    - notify the Nominated Supervisor who will communicate the service's expectation with the family.
- The service name or identity cannot be mentioned in online posts or other online commentary, either directly or implied.
- Employees should not discuss or disclose work-related matters in any public forum.

Legal and Regulatory Foundation

In preparing and implementing this policy, the Approved Provider recognises the obligations and requirements related to –

National Quality Framework

- **Education and Care Services National Law:**
  - s.167 Offence relating to protection of children from harm and hazards
- **Education and Care Services National Regulations:**
  - R.85 Incident, injury, trauma and illness policies and procedures
  - R.86 Notification to parents of incident, injury, trauma and illness
  - R.168 Education and care service must have policies and procedures
  - R.170 Policies and procedures to be followed
  - R.171 Policies and procedures to be kept available
  - R.174A Prescribed information to accompany notice
  - R.175 Prescribed information to be notified to Regulatory Authority
- **National Quality Standard:**
  - QA2 – Children's health and safety
  - QA4 – Staffing arrangements
  - QA5 – Relationships with children
  - QA6 – Collaborative partnerships with families and communities.

Additional Regulatory Context and Guidance

- Working with Children (Risk Management and Screening) Act 2000 (Qld)
- Criminal Code Act 1899 (Qld)
- Online Safety Act 2021 (Cth)
- eSafety Commissioner - Best Practice Framework for Online Safety Education
- eSafety Commissioner - eSafety Early Years program for educators
- National Model Code for Early Childhood, Education and Care.

Date of Development	Reason for Modification	Date Ratified	Date of Review
11.06.24	Adopted new Policy		
	Added National Model Code for ECEC	19.08.24	