

## **G.9 Safe use of digital technologies and online environments**

### **G.9.1 Introduction and Overview**

#### **Policy Statement**

Children's safety and wellbeing are paramount at our service, as we strive to create a safe and positive environment for all children. Part of maintaining such an environment includes putting processes in place to ensure the safe use of digital technologies and online environments.

LOOSH is committed to creating a safe and supportive digital environment for all children. We aim to foster digital literacy while protecting children from potential online risks, such as harmful or illegal content, cyberbullying, and breaches of privacy. We promote respectful digital behaviour and encourage children to develop a healthy relationship with technology.

The purpose of this policy is to establish clear guidelines for the safe and responsible use of digital technologies and online environments at LOOSH. We recognise the value of digital tools in supporting learning and recreation but are equally aware of the potential risks they pose. This policy aims to ensure that all digital interactions involving children are positive, developmentally appropriate, and free from harm.

#### **Background**

The Education and Care Services National Regulations require approved providers to ensure their services have policies and procedures in place for the safe use of digital technologies and online environments at the service. Additionally, with the relevance of technology and the increasing frequency of its use in day-to-day life, the service felt it was important to include policies and procedures outlining practices for safe use.

#### **Guiding Principles**

- All children attending our service are provided with a safe environment through the creation and maintenance of a child safe culture, and this extends to the safe use of digital technologies and online environments
- Children's wellbeing is paramount, and children will be actively involved in decision-making about the safe use of digital technologies and online environments at the service, including taking, using and sharing an image or video of them on a digital device, whether by an adult or a child
- Management, educators, and staff are aware of their roles and responsibilities to identify and respond to every child at risk of child abuse or maltreatment, including abuse or maltreatment that may occur through digital technologies and online environments
- Approved providers, nominated supervisors, educators, volunteers and students, take reasonable precautions and use adequate supervision to ensure children are protected from harm that may occur through digital technologies and online environments

#### **Scope**

This policy applies to all individuals involved in the operation of the service, including children, educators, casual and permanent staff, volunteers, students, families, and any external service providers. It covers the use of all digital technologies, including computers, tablets, smartphones, smartboards, televisions, cameras, and any internet-connected devices.

### **G.9.2 Procedures**

#### **Use of digital devices at the service**

LOOSH uses digital technology and electronic devices for the following purposes:

- As a tool for children's learning

- To document their learning and development
- Communication with families and the wider community
- Communication between staff
- Program planning
- Administration tasks
- Management of compliance
- Storage of documentation and records
- To keep accurate attendance records
- To keep accurate enrolment records.

Educators and staff at our service are responsible for ensuring that all digital technology use is purposeful, developmentally appropriate, and always supervised. Children's access to digital technology is limited to structured activities and is not used as a substitute for play or educator engagement. Educators model respectful digital behaviour and will actively engage with children during digital activities, using these moments as opportunities to discuss online safety and responsible use. All child use of digital technology at the service will be directly supervised by an educator.

Parents and carers will be informed as to how digital technologies are used at the service and will be provided with information regarding the expectations for use. Parents will also be provided with resources about online safety and digital wellbeing as is needed.

#### Acceptable devices

Staff will be provided with devices relevant to their role and duties. Staff will use service devices appropriately and for work-related purposes only.

Staff are prohibited from using or being in possession of personal devices when providing education and care and working directly with children. Exceptions will be made at the discretion of the Nominated Supervisor or delegate, as required but only where access does not impede the active supervision of children and support of their engagement within the program. Such exceptions may include but are not limited to offsite excursions, emergency situations, health and safety reasons or technology failure.

Children are not permitted to use social media, messaging platforms, or personal email accounts while attending the service. Instead, they are encouraged to ask questions, express concerns, and talk openly about their digital experiences. Personal devices (e.g., smartphones, smartwatches) brought by children are not to be used during service hours unless authorised by a parent and approved by staff. Should a child bring a digital device to the service, it will be kept in the LOOSH office until the child is collected.

#### Taking images of children

Written consent will be obtained from parents and carers upon enrolment, to seek their permission to have images or videos captured of their children for the purpose of documenting and sharing learning with families. This consent will be confirmed or updated annually or when circumstances change. The service respects the right of parents and carers to refuse or withdraw photo consent at any time and staff will always ensure that children have the right to say no to being photographed, even if consent has been obtained from their parent or carer. The service will ensure that they communicate with staff which children do not have photo permission and will place every precaution in place to ensure that children with no photo permission can be easily identified. Only service issued electronic devices should be used when taking and storing images or videos of children while providing education and care.

#### Device security

All service devices will be password protected and locked when not in use. Devices will not be left unattended in areas accessible to children, visitors or the public.

On devices used by children, LOOSH will use content filters and security settings where appropriate to reduce access to harmful or inappropriate materials. Only approved websites and applications that align with the service's educational and recreational goals are permitted. Children are not permitted to log into personal accounts (email, social media, YouTube, etc.) on service devices.

### Management of records

The service will take every precaution to ensure that all data collected and stored by the service is managed securely, ethically, and in compliance with legal and regulatory requirements. The service will only collect data necessary for the delivery of quality care and to meet legal obligations outlined in the Early Childhood Education and Care National Law and Regulations. Families will be informed of what data is collected and how it is to be used by the service.

All digital records will be stored in a secure cloud and will be password protected. While LOOSH endeavours to store all records digitally, any physical records will be stored in a locked cabinet, located in the LOOSH office. Access to secure records will only be accessible to upper management and should staff be required to access such records to fulfill their role, permission must be obtained from the Nominated Supervisor prior to them receiving access. Information obtained from these records will remain confidential, with staff only using the data for the purpose of which it was collected.

Should the service become aware of information relating to the safety, welfare or wellbeing of a child or young person in their care, the service will share relevant information with prescribed bodies. The service will ensure that all information exchanged adheres to the criteria outlined under Chapter 16A of the Children and Young Persons (Care and Protection) Act 1998. Information that does not fall within such scope will not be shared with external agencies unless written consent is obtained from the family.

The service will only retain records for the period of which is required by the law. Following the period of retention, any physical records will be shredded, and digital files will be securely deleted. A review of the storage and retention of records will be undertaken regularly by the service to ensure best practice.

### Assessment and management of risks

LOOSH will assess all risks associated with the use of digital technologies and identify mitigation strategies to decrease the likelihood of children being exposed to harm. A risk assessment will be prepared by the service, and all staff will read and acknowledge this document. The risks and mitigation strategies outlined in the risk assessment, will be reviewed annually or in the event that new risks are identified.

### Reporting and incident response

If a child is exposed to or reports an unsafe online interaction, staff will respond immediately by documenting the incident and notifying the Nominated Supervisor. Parents or guardians and relevant authorities will be informed if and when appropriate. The service will follow all relevant reporting requirements in accordance with our Child Protection and Child Safe policies and procedures. Additionally, the service will follow the guidelines for reportable conduct when reporting serious incidents to the Regulatory Authority. In such a case, where a child is involved in an unsafe online interaction at the service, families will be referred to relevant support agencies.

Any loss, theft, damage, data breaches or the misuse of a service device, must be reported immediately to the Nominated Supervisor. The Nominated Supervisor will follow the service performance management and disciplinary action policies and procedures in addition to following relevant reporting protocols as is needed.

### Training and awareness

All educators will receive annual training and induction on the safe use of digital technology at the service. Training and induction materials will be updated as technology and legal requirements evolve.

## G.9.3 Roles and Responsibilities

## Approved provider and Nominated Supervisor

- Ensure that obligations under the Education and Care Services National Law and National Regulations are met
- Ensure that the Safe use of digital technologies and online environments policy and procedures are implemented, the appropriate risk assessments and action plans are completed, and all identified actions are taken to minimise the risks to children's health and safety
- Promote a culture of child safety and wellbeing that underpins all aspects of the service's operations (including online learning environments), to reduce risk to children (including the risk of abuse)
- Ensure the safe use of digital technologies, including smart toys, and online environments at the service
- Ensure nominated supervisors, educators and staff implement practices that align with the National Model Code and the service's child safe practices for the use of electronic and digital devices for taking images or videos of children
- Ensure policies and procedures promote equity and respect diversity for the safety and wellbeing of children and young people
- Take reasonable steps to ensure that nominated supervisors, educators and staff follow the Safe use of digital technologies and online environments policy and procedures
- Ensure that copies of the policy and procedures are readily accessible to nominated supervisors, coordinators, educators, staff, families, and are available for inspection
- Notify families at least 14 days before changing the policy or procedures if the changes will:
  - affect the fees charged or the way they are collected or
  - significantly impact the service's education and care of children or
  - significantly impact the family's ability to utilise the service
- Implement the Safe use of digital technologies and online environments policy and procedures and ensure that any plans developed from risk assessments are in place for individual children and are carried out
- Ensure staff understand how to actively supervise children while using digital technologies
- Meeting staff to child ratios to ensure adequate supervision
- Ensure all educators and staff know where to access the Safe use of digital technologies and online environments policy and procedures
- Have ongoing communication with educators and staff about their responsibilities and any changes to policies, procedures and legislation, particularly as digital technologies evolve quickly
- Support educators and staff to uphold the service's culture of child safety and wellbeing, including when accessing digital technologies and online learning environments
- Support educators and staff to understand the National Model Code and manage the use of electronic and digital devices at the service, including the service's expectations around the use of personal and service issued devices
- When required, work collaboratively with appropriate services and/or professionals to support children's access, inclusion and participation in the program, including their safe access to online learning environments.
- Ensure that personal information or photos will be destroyed or de-identified when no longer needed for the purpose it was collected
- Construct Risk Assessments for safe use of digital technology and online environments, ensure all staff have read, acknowledge and implement strategies to mitigate associated risks
- Incorporate a Technology Code of Conduct in the LOOSH Service Child Safe Code of Conduct

## Educator Responsibilities

- Implement the Safe use of digital technologies and online environments policy and procedures and ensure that any action plans for individual children are carried out
- Implement the service's culture of child safety and wellbeing, including when accessing digital technologies and online learning environments

- Know the individual needs and action plans for the children in your care, and understand how they relate to the safe use of digital technologies and online environments
- Know the children at the service who have photo permission and those who do not consent to having their photo taken.
- Ensure active supervision of children when they are using digital technologies, including by monitoring and maintaining staff to child ratios
- Recognise and respond effectively to children and young people when discussing the use of digital technologies and online environments, considering diverse needs and interests
- Ensure children and young people participate in decision-making in matters affecting them regarding the safe use of digital technologies and online environments at the service
- Educators are to respect the decisions of children and their families and will not take photo or video of a child without their permission. Educators will respect children's choice and autonomy and will not pressure or persuade a child to have their photo taken under any circumstances.
- Ensure you understand the National Model Code and the service's expectations around the use of personal and service issued devices while at the service and seek guidance when needed from the nominated supervisor or approved provider.
- Ensure that personal information or photos will be destroyed or de-identified when no longer needed for the purpose it was collected
- Read and implement strategies from the Risk Assessment for safe use of digital technologies and online environments

#### **Parent/carer Responsibilities**

- Adhere to the Safe Use of Digital Technologies and Online Environments Policy and associated procedure
- Indicate as required whether they consent to photos or videos of their child to be taken for the purpose of documenting learning.
- Not use personal electronic devices to take photos, record audio, or capture video of children being educated and cared for at LOOSH
- Be aware that sometimes other children at LOOSH may feature in the same photos, videos, and/or observations as their children. In these cases, families are never to duplicate or upload them to the internet/social networking sites or share them with anyone other than family members.
- Report any concerns related to child safety, including inappropriate use of digital technology, to the approved provider or nominated supervisor

#### **G.9.4 Legislation and Related Service Documentation**

##### **Legislative requirements:**

- Children and Young Persons (Care and Protection) Act 1998 (NSW)
- Education and Care Services National Law sections 162A, 165, and 167
- Education and Care Services National Regulations 84, 122, 123, 168, 170, 175
- Standards 1.1, 1.2, 1.3, 2.1, 2.2, and 7.1 of the National Quality Standard
- Australian Privacy Principles
- eSafety Commissioner Guidelines
- Taking Images or Videos of Children while providing early childhood education and care – ACECQA National Model Code
- United Nations Convention on the Rights of the Child
- Australia's National Principles for Child Safe Organisations

### Related Service Documentation and Policies:

- Incident, Injury, Trauma, and Illness forms
- Child Safe Code of Conduct
- LOOSH commitment to child safety
- Expectations for Communication Policy
- Child safe policy
- Child Protection Policy
- Privacy and Confidentiality Policy
- Behaviour Management Policy
- Management of Incident, Injury, and Trauma Policy
- Quality Program and Practice Policy
- Induction, Training and Professional Development Policy
- Performance Management Policy
- Disciplinary Action Policy

### G.9.5 Key Terminology

| Term                 | Meaning                                                                                                                                                                                                                                                                                                                                           | Source                                         |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|
| Confidentiality      | Keeping information shared by an individual private, without disclosing the information to others.                                                                                                                                                                                                                                                | Legal dictionary                               |
| Cyberbullying        | When someone uses the internet to be mean to a child or young person, so they feel bad or upset.                                                                                                                                                                                                                                                  | NQF Child Safe Culture and Online Safety Guide |
| Harmful content      | Harmful content includes: <ul style="list-style-type: none"><li>• sexually explicit material</li><li>• false or misleading information</li><li>• violence</li><li>• extremism or terrorism</li><li>• hateful or offensive material.</li></ul>                                                                                                     | NQF Child Safe Culture and Online Safety Guide |
| Illegal Content      | Illegal content includes: <ul style="list-style-type: none"><li>• images and videos of child sexual abuse</li><li>• content that advocates terrorist acts</li><li>• content that promotes, incites or instructs in crime or violence</li><li>• footage of real violence, cruelty and criminal activity.</li></ul>                                 | NQF Child Safe Culture and Online Safety Guide |
| National Law         | The applied law system sets a national standard for children's education and care across Australia.                                                                                                                                                                                                                                               | Guide to the NQF                               |
| National Regulations | The Regulations support the National Law by providing detail on a range of operational requirements for an education and care service.                                                                                                                                                                                                            | Guide to the NQF                               |
| Nominated Supervisor | In relation to an education and care service means, a person who: <ul style="list-style-type: none"><li>• Is nominated by the approved provider of the service under Part 3 to be a Nominated Supervisor of that service; and</li><li>• Unless the individual is the approved provider, has provided written consent to that nomination</li></ul> | National Law                                   |
| Online Environments  | the digital space facilitated by the internet or a local network where users can interact, learn, and share information                                                                                                                                                                                                                           | NQF Child Safe Culture and Online Safety Guide |

|                      |                                                                                                                                                                                                                                                                                                                                                                                        |                              |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| Regulatory Authority | A person declared by a law of a participating jurisdiction to be the regulatory authority for that jurisdiction or for a class of education and care services for that jurisdiction                                                                                                                                                                                                    | National Law                 |
| Reportable conduct   | Certain organisations or entities have legal obligations under Reportable Conduct Schemes. Under these Schemes, certain organisations or entities are required to notify and investigate certain allegations (reportable allegations) of abuse involving a child, when the allegation is against someone they employ, engage or contract in circumstances outlined by the legislation. | Child protection legislation |
| Risk assessment      | Assessing the risk means working out how likely it is that a hazard will harm someone and how serious the harm could be.                                                                                                                                                                                                                                                               | ACECQA                       |

|                                       |                |
|---------------------------------------|----------------|
| <b>Date endorsed</b>                  | 29 August 2025 |
| <b>Date for review and evaluation</b> | 29 August 2028 |