QA2 Safe Use of Digital Technologies and Online Environments Policy

NATIONAL QUALITY STANDARDS (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.
2.2.3	Child Protection Child Safety and Protection	Management, Educators and Team Members are aware of their roles and responsibilities regarding child safety, including the need to identify and respond to every child at risk of abuse or neglect. Management, educators and staff are aware of their roles and responsibilities regarding child safety, including the need to identify and respond to every child at risk of abuse or neglect.
QUALITY AREA 7 GOVERNANCE AND LEADERSHIP		
7.1.2	Management System	Systems are in place to manage risk and enable the effective management and operation of a quality service that is child safe.

EDUCATION AND CARE SERVICES NATIONAL LAW AND REGULATIONS	
S162A	Child protection training
S165	Offence to inadequately supervise children
S.166A	Once to subject child to inappropriate conduct (NSW)
S167	Offence relating to protection of children from harm and hazards
12	Meaning of a serious incident
73	Educational Program
76	Information about educational program to be given to parents
84	Awareness of child protection law
115	Premises designed to facilitate supervision
122	Educators must be working directly with children to be included in ratios
123	Educator to child ratios – centre-based services
149	Volunteers and students
155	Interactions with children
156	Relationships in groups
165	Record of visitors
166	Children not to be alone with visitors
168	Education and care services must have policies and procedures
18(2)(ha)	The safe use of digital technologies and online environments at the service
170	Policies and procedures to be followed
171	Policies and procedures to be kept available
172	Notification of change to policies or procedures
175	Prescribed information to be notified to Regulatory Authority
176	Time to notify certain information to Regulatory Authority
181	Confidentiality of records kept by approved provider
183	Storage of records and other documents
184	Storage of records after service approval transferred

RELATED POLICIES AND RECORDS

Dealing with Complaints Policy	Educational Program & Practice Policy
Enrolment and Orientation Policy	Child Safe Organisation Policy
Using Technology to Enhance the Educational Program Policy	Active Supervision Policy
Relationships with Children Policy	Governance and Management Policy
Record Keeping and Retention Policy	Staffing Arrangements Policy
Student, Agency, Educators, Visitors and Volunteers Policy	Social Media Policy
Code of Conduct Policy	Child Protection Policy
Incident, Injury, Trauma and Illness Policy	Privacy and Confidentiality Policy
Reporting to the Regulatory Authority Policy	CCTV Policy
Electronic Service-Supplied Device Register	Digital Device Exemption Request Form

AIM OF POLICY

Our service is committed to fostering a culture that creates and maintains a safe online environment with support and collaboration from staff, families and community. As a child safe organisation, our Service embeds the National Principles for Child Safe Organisations and continuously addresses risks to ensure children are safe in physical and online environments. Digital technologies have become an integral part of many children's daily lives. For this reason, it is important that our educators are not only familiar with the use of digital technologies, but are able to guide children's understanding of, and ability to interact, engage, access and use a range of digital technology in a child safe environment.

PURPOSE

Children's safety and wellbeing are paramount, and our service has the responsibility to provide and maintain a safe and secure working and learning environment for staff, children, visitors and contractors, including online environments. We aim to create and maintain a positive digital 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.

The use of closed-circuit television (CCTV) installed at the service aims to address crime prevention strategies to reduce concerns, deal with complaints and support investigations. Our service adheres to the Privacy Act 1988 (Privacy Act) and complies with the Australian Privacy Principles.

The Education and Care Services National Regulations require Approved Providers to ensure the service has a policy in place for the safe use of digital technologies and online environments at the service.

SCOPE

This policy applies to children, families, team members, agency educators, management, and visitors to our Story House services.

OUR APPROVED PROVIDER WILL ENSURE

- The *Safe Use of Digital Technologies and Online Environments Policy* is reviewed and maintained by management and always adhered to by educators and team members.
- Those obligations under the Education and Care Services National Law and National Regulations are met.
- They take reasonable steps to ensure that the policy and procedures are current, reviewed regularly, and communicated to educators, team members and stakeholders.
- They take reasonable steps to inform and support educators and team members regarding their responsibilities in always implementing the policy and procedures.
- They take reasonable steps to ensure that Service Managers, educators, team members agency educators and volunteers follow the policy and procedures.
- Copies of the policy and procedures are readily accessible to Service Managers, educators, team members, stakeholders and volunteers and are available for inspection.
- They 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.

OUR SERVICE MANAGER WILL ENSURE

- New team members, students and volunteers are provided with a copy of the *Safe Use of Digital Technologies and Online Environments Policy* as part of their induction and are advised on how and where the policy can be accessed
- All team members, educators, volunteers and students are aware of current child protection law, National Principles for Child Safe Organisations and their duty of care to ensure that reasonable steps are taken to prevent harm to children
- Families are aware of this *Safe Use of Digital Technologies and Online Environments Policy* and are advised on how and where the policy can be accessed
- They promote and support a child safe environment, ensuring adherence to the *Child Safe Environment and Child Protection Policies,* including mandatory reporting obligations
- The National Principles for Child Safe Organisations is embedded into the organisational structure and operations
- Professional learning is provided to educators and staff relating to the safe use of digital technologies and online environments
- all electronic devices purchased and supplied for the Service are recorded via the *Electronic Service-Supplied Device Register*
- an *Electronic Service-Supplied Device Register* is developed and monitored for all electronic devices purchased and used at the Service
- Appropriate ratios and adequate supervision are maintained for children at all times including when using digital technology and accessing online environments
- Students, volunteers and/or visitors are never left alone with a child whilst at the Service under any circumstances
- All team members, educators, volunteers and students are aware of the National Model Code and Guidelines and adhere to these recommendations for taking images or video of children including:
- Personal electronic devices or personal storage devices, that can take images or videos, are not used by educators, staff, visitors or volunteers when working directly with children
- Team members and educators only use electronic devices issued by the Service for taking images or videos of children enrolled at the Service

VISITORS AND VOLUNTEERS WILL

- adhere to the Safe Use of Digital Technologies and Online Environments Policy whilst visiting the Service
- not use personal electronic devices, such as mobile phones smart watches or META sunglasses, to take photos, record audio, or capture video of children being educated and cared for at the Service without written permission.

- Service supplied or issued devices are securely configured, monitored and maintained to prevent unauthorised access
- exemptions for prescribed circumstances are authorised, in writing, for staff to possess or control a personal device while working directly with children
- Visitors who are supporting children at the Service (NDIS funded support professionals, Inclusion Support Professionals) obtain written authorisation from families to capture images or video of a child for observation/documentation purposes only
- Children, educators and families are aware of our Service's complaints handling process to raise any concerns they may have about the use of digital technologies or any other matter, as per the *Dealing with Complaints Policy*
- The Service *Privacy and Confidentiality Policy* is always adhered to by team members, educators, families, visitors, volunteers and students
- Families are informed of how the Service will take, use, store and destroy images and videos of children enrolled at the Service during enrolment and orientation
- Written authorisation is requested from families to take, use, store and destroy digital documentation including images and videos of children
- Images or videos of children are not taken, used or stored without prior parent/guardian authorisation
- Written authorisation is obtained from parents/guardians to collect and share personal information, images or videos of their children online e.g. Website, Facebook, Instagram or Storypark
- Families are informed to withdraw authorisation, a written request is required
- Digital images and videos for individual children are deleted or destroyed and removed from storage when authorisation has been revoked from the parent/guardian
- They review how images and videos are stored on a regular basis and ensure new educators and staff have access to relevant folders and files, if required, in accordance with their role
- Digital data is stored securely, whether offline or online, using a cloud-based service, and that data is archived regularly
- Images and videos are deleted or destroyed and removed from storage devices in accordance with the *Record Keeping and Retention Policy,* images and videos used for documenting children's learning and development must be kept as per this policy
- External agencies or specialists are consulted if concerns are identified relating to online abuse, cyberbullying or digital safety risks

	• Policies and procedures reflect a commitment to equity and diversity, protect children's privacy, and empower children to be independent • Collaboration with relevant professionals, as required, to support equitable access to digital technologies for all children • They remain informed of privacy legislation through monitoring of updated from relevant government authorities such as the Office of the Australian Information Commissioner (OAIC) • A risk assessment is conducted regarding the use of digital technologies by staff and children at the Service, including accessing online environments • Risk assessments for digital technology and online environments are reviewed annually or as soon as possible after becoming aware of any circumstances that may affect the safety, health or wellbeing of children • Policies and procedures are reviewed following an identification of risks following the review of risk assessments relating to the use of digital technologies and online environments • Team members, educators, families and children are informed of updates to policies, procedures or legislation relating to digital technologies and online environments • A review of practices is conducted following an incident involving digital technologies or online environments, including an assessment of areas for improvement • Educators are informed of, and adhere to recommended timeframes for 'screen time' according to *Australia's Physical Activity and Sedentary Behaviour Guidelines* • They share information to families about recommended screen time limits based on *Australia's Physical Activity and Sedentary Behaviour Guidelines.*

OUR EDUCATORS WILL ENSURE

- They adhere to the *Safe Use of Digital Technologies and Online Environments Policy.*
- They are aware of current child protection law, National Principles for Child Safe Organisations and their duty of care to ensure that reasonable steps are taken to prevent harm to children
- They promote and support a child safe environment, ensuring adherence to the *Child Safe Environment* and *Child Protection Policies,* including mandatory reporting obligations
- They participate in practical training related to digital safety, privacy protection and responsible use of technology
- They understand the critical importance of implementing active supervision strategies when children are accessing online environments to keep children safe
- They promote and contribute to a culture of child safety and wellbeing in all aspects of our Service's operations, including when accessing digital technologies and online learning environments
- They do not use, or have access to, any personal electronic devices, including mobile phones or smart watches used to take images or video of children at the Service, unless an exemption has been authorised.
- Not breach children and families' privacy
- They keep passwords confidential and log out of computers and software programs after each use
- They ask permission before taking photos of children on any device and explain to children how photos of them will be used and where they may be published
- They ensure children's personal information where children can be identified such as name, address, age, date of birth etc. is not shared online
- They ensure that screen time is NOT used as a reward or to manage challenging behaviours under any circumstances
- They introduce concepts to children about online safety at age-appropriate levels
- They support children's understanding of online safety by providing age-appropriate guidance, discussions and activities that help them to recognise safe and unsafe online behaviours
- They consult with children about matters that impact them, including the use of digital technologies and online environments, to ensure their voices are heard and respected in a meaningful way.

FAMILIES WILL ENSURE

- They adhere to the *Safe Use of Digital Technologies and Online Environments Policy*
- They do not use any personal electronic devices, including mobile phones or smart watches to take images or video of children at the Service,
- They are aware that sometimes other children in the Service 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.
- They seek permission from the Service Manager and communicate any requirement for a device that their child may need to use for their development or to communicate with educators where their child may be non-verbal.
- That any school aged child understands that they may not use their personal device while cared for at the service, and that any personal device must be placed in a secure location, away from other children.

Safety – We value the delivery of safe places for the mental and physical wellbeing of all.

IMPLEMENTATION

DOCUMENT TITLE	**Safe Use of Digital Technologies and Online Environments Policy**			**VERSION**	V2
DATE PUBLISHED	August 2025	**Last review**	February 2026	**Next review**	February 2027
APPROVED BY	Chief People Officer		**OWNER**	People & Culture	
Warning – uncontrolled when printed. This document is current at the time of printing ©Story House Early Learning					

Our Service uses digital technology and electronic devices as a tool for learning with children, documenting their learning and development, communicating with families and the wider community, supporting program planning and administration tasks and enhancing safety and security through systems such as sign in/out platforms and CCTV monitoring. Our educators are diligent in ensuring children are only able to access age-appropriate technology on a service-issued device.

DIGITAL TECHNOLOGY AND ELECTRONIC DEVICES USED AT THE SERVICE

Our Service follows the National Model Code and Guidelines for taking images or videos of children. Our Service ensures compliance with the Education and Care Services (Supply, Authorisation and Use of Devices) Order 2025 (NSW only)

The use of personal electronic devices used to take, store or transfer images or videos of children who are being educated and cared for at the Service is strictly prohibited. Personal electronic devices include items such as tablets, mobile phones, computers/laptops, digital cameras, smart watches, META sunglasses (wearables) and personal storage and file transfer media (such as SD/memory cards, USB drives, hard drives and cloud storage) and other new and emerging technologies.

Staff and educators are advised that electronic devices supplied or issued by and registered with the Service must not be removed from the premises as they may contain personal details of staff or children, including photos or videos. Exemptions may apply when required for operational activities, for example excursions or transportation.

EXEMPTIONS

There are limited circumstances where personal devices are allowed to be used while a person is working directly with children. These circumstances include:

- During a service's excursion with children, when a personal device is necessary for the safety of or to support the education and care of children in the service. Educators will not use these personal devices to take photos, record audio, or capture video of children being educated and cared for at the Service without written permission.
- While children are being transported by the service or on transportation arranged by the service. Personal devices are allowed only when they are considered necessary for the safety of or to support the education and care of children in the service.
- Specific personal device use if written authorisation is given by the approved provider.

Written authorisation may be given to authorise a team member to use a personal device, including a phone, tablet or smartwatch, while working directly with children if they determine that it is necessary for the following reasons:

- Providing support or assistance with the person's disability or health needs, with supporting documentation from a medical practitioner
- Communication with a family member of the person. This should only be used in limited circumstances where a person's family member requires immediate communication, and it is not practical to contact the person via the service's phones
- Where a service-supplied device ceases working (and a device is needed for the safety of children or the provision of education and care to children).
- In a service-based emergency (e.g. missing child, lockdown, evacuation or injury) or local emergency event to receive alerts (e.g. government bushfire or evacuation notifications).
- For work, health and safety reasons.

Team members must request authorisation via Story House's digital request form, and the request must be reviewed by the Service Manager. Authorisation must be given in advance for the above purposes, except in circumstances where it is not practical to give prior authorisation. This may include emergency situations such as a lock down or a bush fire where it is not safe or realistic for an approved provider to give written authorisation prior to use of the personal device.

Children enrolled at our service are not permitted to bring electronic devices to the service, unless an exception has been discussed with the Approved Provider or Nominated Supervisor where the device may be required to support a diagnosed medical condition or disability or is used for the purposes of communication in non-verbal children.

Additional practices for NSW Services only:

Exemptions for prescribed circumstances must be reviewed every 3 months. Written authorisations must be retained for a period of 3 years. An additional prescribed circumstances may apply if a Service-supplied or issued device stops working and another device is temporarily required. Approved providers may revoke authorisations as required, ensuring that all revocations are properly documented. Written prescribed circumstance authorisations must include Service details, person's details, reasons for the authorisation and duration of the authorisation.

SERVICE-SUPPLIED OR ISSUED ELECTRONIC DEVICES

Service-supplied or issued devices must be configured to comply with SHEL policies and procedures as outlined within this policy. Services will maintain records of electronic Service-supplied devices. Including the date of supply, type of device, make, model, serial number, name and signature of approved provider supplying the device and a declaration that the device is configured to operate in line within this policy. If the device is no longer used within the Service, a record of revocation will be documented. Devices recorded in the register may include, but are not limited to, computers, tablets, mobile phones, cameras, CCTV systems, audio recorders, smart toys, baby monitors and any other internet-connected or data-enabled devices used within the Service. Electronic devices supplied or issued by and registered with the Service will be stored in a locked cabinet at the end of the day. Records relating to the supply or issue of electronic devices, including registers of use Service-supplied or issued device is to be stored securely for a period of 3 years from the date the record was made.

IMAGES AND VIDEOS

The Approved Provider is responsible for determining who is authorised to take, use, store and destroy images and videos of children using service-supplied or issued digital devices. Images and videos will be stored securely with password protection, with access limited to authorised personnel only. Images and videos of children must only be taken and used in accordance with service policies, and careful consideration given to the purpose of the image or video. Educators will engage in discussions that consider the intent, appropriateness, context and consent involved in capturing and using the images and videos, ensuring the process aligns with children's learning, wellbeing and right to privacy.

Our service will regularly review how digital data, including images and videos of children, is stored. Back-ups of all digital data, whether offline or online (such as a cloud-based service), will be regularly performed. Digital data stored at the service will be destroyed in accordance with the *Record Keeping and Retention Policy*. The Approved Provider will ensure staff, agency educators, educators, visitors and volunteers do not transfer images or videos from service issued devices to personal devices. Unauthorised transferring of digital data may result in disciplinary action.

PHYSICAL ENVIRONMENT AND ACTIVE SUPERVISION

The approved provider, nominated supervisor, management and educators will:

- ensure children are always supervised and never left unattended whilst an electronic device is connected to the internet
- provide a child safe environment to children- reminding them if they encounter anything unexpected that makes them feel uncomfortable, scared or upset, they can seek support from staff
- reflect on our service's physical environment, layout and design to ensure it supports child safe practices when children are engaged in using technology
    - perform regular audits to identify risks to children's safety and changes in room set-ups that can indicate areas of higher-risk and become supervision 'blind spots'
    - ensure location of digital technology/equipment allows educators to remain in line-of-sight of other staff members when working with children
    - only permit children to use devices in open areas where educators can monitor children's use

- be aware of high-risk behaviours for children online, including uploading private information or images, engaging with inappropriate content (inadvertently or purposefully), making in-app purchases, and interacting with unsafe individuals
- ensure all visitors and volunteers are always supervised
- ensure all devices are password protected with access for staff only

- where digital devices are used during transportation and excursions, they must be used in accordance with practices outlined within this policy.

SOFTWARE PROGRAMS AND APPS

Our service uses a range of secure software programs and apps on service-supplied or issued devices to support the educational program and administration of the service. All apps used by staff, educators, visitors and children are carefully selected, regularly checked and kept up to date with the latest available system updates. Access to software programs and apps is password-protected to ensure the privacy of children, families and staff. Each user is required to create their own user account and ensure log in, and password information is not shared.

The Approved Provider will ensure programs that require additional background checks, such as CCS Software, are only accessed by authorised staff who have completed necessary screening processes in accordance with Family Assistance Law. Educators use our educational program software to share observations, photos, videos, daily reports, and learning portfolios with families in a secure, closed platform.

ARTIFICIAL INTELLIGENCE (AI) INTERACTIONS AND GUIDELINES

Educators or staff using AI are to be aware of limitations, privacy risks, and the potential for errors in the information it provides. AI can support and assist staff as a documentation tool; however, it is their responsibility to ensure the information's accuracy and not rely upon it as an authoritative source. Staff and educators should ensure they enter original work into the AI program and are required to monitor, verify, and check information obtained from AI to ensure specific details are contextually relevant. Data and privacy concerns must be addressed, and staff should not enter details that may identify individual children, such as names and date of birth.

CONFIDENTIALITY AND PRIVACY GUIDELINES

Our *Privacy and Confidentiality Policy* applies to all use of digital technology and online environments.
All staff, educators, and visitors must ensure that any information, images, or digital content related to children, families, and the service is collected, stored, used, and shared in accordance with privacy legislation and service procedures, to maintain confidentiality and protect the safety and wellbeing of children. The nominated supervisor will advise the approved provider as soon as possible regarding any potential threat to security information and access to data sensitive information.
Our Service will follow practices to protect personal and sensitive digital data.
The Approved Provider will notify the Office of the Australian Information Commissioner (OAIC) in the event of a possible data breach by using the online Notifiable Data Breach Form. This could include:

- 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
- ensure educators are aware of their mandatory reporting requirements and report any concerns related to child safety including inappropriate use of digital technology or inappropriate conduct to the approved provider or nominated supervisor.

IDENTIFICATION AND REPORTING OF ONLINE ABUSE AND SAFETY CONCERNS

Our Service will implement measures to keep children safe whilst using digital technology and accessing online environments.
The approved provider, nominated supervisor and management will -

- ensure all staff, educators, students and volunteers are aware of their mandatory reporting obligations and promptly report any concerns related to child safety, including inappropriate use of digital technology, to the approved provider or nominated supervisor, aligned with the *Child Protection Policy*.

- support educators to:
  - encourage children to seek support if they encounter anything unexpected that makes them feel uncomfortable, scared or upset
  - listen sensitively and respond appropriately to any disclosures children may make relating to unsafe online interactions or exposure to inappropriate content, adhering to the *Child Protection Policy* and reporting procedures
  - respond to and report any breaches and incidents of inappropriate use of digital devices and online services to management
- ensure all concerns are documented and responded to promptly and appropriately, with support provided to the child and their family as required
- ensure all educators, staff, students and families are advised of the *Whistleblower Policy*, whistleblower protections and processes
- report any suspected cases of online abuse to the relevant authorities, including the eSafety Commissioner and Police, in accordance with legal requirements and child protection procedures
- notify the regulatory authority as per the *Reporting to the Regulatory Authority Policy*, if a child is involved in a serious incident, including any unsafe online interactions, exposure to inappropriate content, or suspected online abuse.

USE OF CLOSED-CIRCUIT TELEVISION (CCTV) MONITORING

Our Service uses CCTV to monitor the physical environment. Our Service will regularly review guidance on the use of surveillance devices, including information provided by the Office of the Australian Information Commissioner.

Our Service does not use baby monitors within the Service. Access to the monitor is restricted through a password-protected system to ensure security and prevent unauthorised viewing. Families are informed the Service uses CCTV as a surveillance method during enrolment and orientation to the Service.

CCTV is installed, used and monitored as per the *CCTV Policy*.

The CCTV recording system operates in real mode, monitoring the site continuously 24 hours a day. Footage and information collected via the recording system will be governed by *Australian Privacy Principles* and all relevant staff will be kept up to date with requirements under Australia's privacy law.

KEY TERMS

Artificial intelligence (AI)	An engineered system that generates predictive outputs such as content, forecasts, recommendations, or decisions for a given sent of human defined objectives or parameters without explicit programming.
Cyberbullying	When someone uses the internet to be mean to a child or young person so they feel bad or upset
Cyber safety	Safe and responsible use of the internet and equipment/devices, including mobile phones and devices.
Disclosure	Process by which a child conveys or attempts to convey that they are being or have been sexually abuses, or by which an adult conveys or attempts to convey that they were sexually abused as a child
Generative artificial intelligence (AI)	A branch of AI that develops generative models with the capability of learning to generate novel content such as images, text and other media with similar properties as their training data
ICT	Information and Communication Technologies
Illegal content	Includes: images and videos of child sexual abuse Content that advocates terrorist acts Content that promotes, incites or instructs in crim or violence Footage of real violence, cruelty and criminal activity
Optical Surveillance Device	Has the same meaning as in section 6(1) of the Surveillance Devices Act 2004 of the Commonwealth

Online hate	Any hateful posts about a person or group based on their race, religion, ethnicity, sexual orientation, disability or gender
Personal device	A personal device is a device that is owned by a person (NOT owned/supplied by an approved provider for education and care purposes) and is capable of capturing, storing or transmitting an image, for example phones, smart watches, cameras, tablet computers, and hard drives (ACECQA).
Smart toys	Smart toys generally require an internet connection to operate as the computing task is on a central server
Sexting	Sending a sexual message or text, with or without a photo or video. It can be done using a phone service or any platform that allows people to connect via an online message or chat function
Unwanted contact	Any type of online communication that makes you feel uncomfortable, unsafe or harassed.

Source: Glossary to NQF Child Safe Culture and Online Safety Guides- ACECQA 2025

CONTINUOUS IMPROVEMENT AND REFLECTION

Our *Safe use of digital technologies and online environments Policy* will be reviewed on an annual basis in consultation with children, families, staff, educators and management. Families will be notified of changes to policies within 14 days to ensure they remain informed and can provide feedback or ask questions as needed

SOURCE

- Australian Children's Education & Care Quality Authority - ACECQA
- Guide to the National Quality Framework. 2020
- Education and Care Services National Law Act 2010.
- National Regulations 2018
- Code of Ethics
- United Convention on the Rights of the Child
- ACECQA Child Safe Culture Guide
- ACECQA Safe Use of Digital Technologies and Online Environments Fact Sheet
- Australian Children's Education & Care Quality Authority. (2025). *Guide to the National Quality Framework*
- Australian Children's Education & Care Quality Authority. (2023). *Embedding the National Child Safe Principles*
- Australian Children's Education & Care Quality Authority. (2024). *Taking Images and Video of Children While Providing Early Childhood Education and Care. Guidelines For The National Model Code*.
- Australian Children's Education & Care Quality Authority. (2025). *NQF Online Safety Guide*
- Australian Government eSafety Commission (2020) www.esafety.gov.au
- Australian Government Department of Education.(2025). *Child Care Provider Handbook*
- Australian Government. eSafety Commissioner Early Years program for educators
- Australian Government, Office of the Australian Information Commissioner. (2019). Australian Privacy Principles: https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/
- Australian Government Department of Health and Aged Care. (2021). Australia's Physical Activity and Sedentary Behaviour Guidelines
- Australian Human Rights Commission (2020). *Child Safe Organisations.* https://childsafe.humanrights.gov.au/