Early Education and Care Services

2.25. eSAFETY FOR CHILDREN

QUALITY AREA 2 I VERSION 2.0

Regulatory Policy & Procedure

Statement of Commitment

Wyndham City Council is committed to safeguarding children younger than 18 and ensuring their active participation as valued members of our community, while fostering a child-safe environment. We focus on early identification of risks to protect children from harm, whether caused by adults, harmful behaviours between children, exposure to family violence, or concerns like grooming, cumulative harm, or neglect.

We encourage the reporting of any concerns or suspicions of child abuse or harm. The Reportable Conduct Scheme improves how organisations respond to allegations of abuse, harm, neglect, and risk to children. Under this scheme, the CEO, or their delegate, must report any allegations of child-related misconduct to the Commission for Children and Young People within a specific timeframe.

All allegations are taken seriously, and reporting does not require agreement on the conduct. Concerns can be reported to a line manager or directly to the Senior Child Safe Advisor. Investigations will be conducted by an external party under the oversight of relevant authorities, including Victoria Police, the Department of Families, Fairness and Housing, and Child Protection.

Furthermore, Wyndham City Council has also publicly declared its commitment to being a Child Safe Organisation on our external website and recognises the importance of Child Safety in the provision of quality community services. All children and young people who attend services, programs, events, and community spaces have a right to feel safe, be safe, and be heard. We are committed to maintain a child safe environment, and value a culture of safety within council and its operations.

There are also behavioural expectations to recognise the importance of an inclusive and welcoming environment to all children & young people of the wider community including Aboriginal and Torres Strait Islanders, culturally and/or linguistically diverse, those with a disability and promoting an environment with no tolerance for racism.

Purpose

This policy explains how we use digital technologies and online spaces in Early Education and Care Services (EECS). Our goal is to support children’s learning, wellbeing, and safety, while protecting their privacy and keeping them safe from harm. It also sets clear guidelines for all stakeholders; approved providers, educators, staff, families, volunteers, and children, to use digital technologies in a safe and responsible way. These guidelines follow the National Quality Framework (NQF), relevant legislation, and best practice.

This policy aims to:

- Promote a child safe culture across all physical and digital spaces.
- Provide a framework for the safe use of digital tools, online environments, and media.
- Establish roles, responsibilities, and practices that reduce risk and support active supervision.
- Communicate with families about safe online practices at home, in services, and in the community.
- Support the rights of children and families to be informed, give consent, and withdraw it.
- Guide staff in identifying and responding to online risks and incidents of harm.

Policy Statement

EECS is committed to:

- Ensuring the safety and wellbeing of all children, educators, families, and visitors, including in digital and online spaces.
- Recognising that digital technologies are valuable tools for education and communication and must be used in a way that promotes a child-safe environment.
- Ensuring we uphold children’s rights to safety, privacy, and dignity when it comes to digital technologies and online environments.
- Advocating and promoting the reduction of children’s digital footprints.
- Fulfilling our duty of care by actively identifying and managing risks of abuse or harm to children.

Scope

This policy applies to the approved provider, persons with management or control, nominated supervisor, persons in day-to-day charge, early childhood teachers, educators, staff, students, volunteers, parents/guardians, children, and any other individuals attending EECS programs and activities, including offsite excursions and digital learning experiences.

For clarification of ***bolded italicised*** terms, please see the Definitions section below.

Responsibilities	Approved Provider and EECS Unit	Nominated Supervisors/ Team Leaders	Early Childhood Teacher, Educators, and other staff	Family, parents/guardians	Contractors, volunteers, and students
1. Ensure all EECS services comply with all relevant legislations and obligations under the *Education and Care Services National Law* and *National Regulations.*	✓	✓	✓		
2. Ensure all staff can access, understand and are compliant with *Policy 2.25: eSafety for Children* and its related processes.	✓	✓	✓		
3. Review this policy in consultation with stakeholders, including parents/guardians.	✓	✓	✓	✓	✓
4. Ensure all digital technology use aligns with related EECS and Wyndham City Council policies, including: • *Policy 4.01 - Code of Conduct* • *Policy 2.01 – Providing a Child Safe Environment* • *Policy 7.03 – Privacy and Confidentiality* • *Appendix 4.01.1 – WCC Corporate Code of Conduct*, • *Appendix 4.02.1 – WCC Values and Behaviours* • *Appendix 2.26.7 – Wyndham Records & Information Management Policy*	✓	✓	✓		✓
5. Create and maintain a culture where child safety and wellbeing are a priority in all areas of EECS, including online environments, to help prevent harm or abuse.	✓	✓	✓	✓	✓
6. Uphold children's rights to safety, privacy, and participation in digital environments.	✓	✓	✓	✓	✓
7. Ensure every service has an appointed Online Safety Champion to be the main contact for reporting online safety issues.	✓	✓			
8. Provide staff with regular opportunities for formal and informal professional learning to stay updated on identifying and mitigating online safety risks and evolving practices. (proposed learning: *eSafety Early Years professional learning modules - refer to Related Appendices & Documents)*	✓	✓			
9. Staff engage in professional learning to build capacity and support the implementation of online safety education.	✓	✓	✓		✓

Responsibilities	Approved Provider and EECS Unit	Nominated Supervisors/ Team Leaders	Early Childhood Teacher, Educators, and other staff	Family, parents/guardians	Contractors, volunteers, and students
10. Document staff professional learning on online safety in staff record forms.	✓	✓	✓		✓
11. Review online safety education annually to identify strengths and weaknesses and update to ensure relevance to online safety issues, risks, and harms	✓	✓			
12. Support staff to identify, manage, and reduce online risks.	✓	✓			
13. Conduct a risk assessment for all ***digital tools, online platforms,*** and ***smart toys*** before they are accessed or used by children. Review annually. *(Appendix 2.25.04: Online Safety Self-Assessment and Risk Assessment Tool)*	✓	✓	✓	✓	✓
14. Ensure risk management plans address the needs of all children, including: • those with disability • Aboriginal and Torres Strait Islander children • ***LGBTQIA+*** students • children from culturally and linguistically diverse backgrounds • children experiencing family breakdown • children in out-of-home care • other vulnerable groups susceptible to online harm	✓	✓	✓		✓
15. When engaging third-party contractors complete a risk assessment that includes the following: • assess whether engagement poses a risk of child abuse or harm. • identify the extent of the risk • strategies to prevent child abuse or harm.	✓	✓	✓		✓
16. Ensure appropriate filtering and monitoring are in place for all devices used at the service.	✓	✓	✓		✓
17. Ensure only Wyndham City Council service-issued electronic devices are used to take photos or record videos of children.	✓	✓	✓	✓	✓
18. Ensure staff and any other individuals do not use personal electronic devices to photograph or record children while educating and caring for them, both in the kindergarten service and during excursions.	✓	✓	✓	✓	✓
19. Proactively manage the taking of photos and videos by others attending or participating in service activities or events.	✓	✓	✓		✓
20. Staff personal electronic devices, that are not required for essential purposes, are to be stored safely away from use while educating and caring for children.	✓	✓	✓	✓	✓
21. Ensure staff do not use or carry ***personal storage devices*** or ***file transfer media*** while providing education and care or working directly with children, unless prior approval has been granted by the Approved Provider. *(refer to Process 2.25.4 – Apply for Approval to Use Personal Device)*	✓	✓	✓		✓

Responsibilities	Approved Provider and EECS Unit	Nominated Supervisors/ Team Leaders	Early Childhood Teacher, Educators, and other staff	Family, parents/guardians	Contractors, volunteers, and students
22. Ensure that any exceptions to staff using or carrying personal storage devices or file transfer media are: - limited to essential purposes only - are authorised in writing by the Approved Provider (or through another appropriate means if written approval is not reasonably practicable) - and do not compromise the active supervision and safety of children *(Appendix 2.25.08 – Application Form: Use of Personal Device)*	✓	✓	✓		✓
23. Ensure there are clear procedures for capturing, storing and sharing of children's images and videos *(refer to Policy 7.03 – Confidentiality and Privacy)*	✓	✓	✓	✓	✓
24. Obtain children's verbal or non-verbal consent before taking images or videos *(refer to Process 2.25.2: Photo and Video consent for children under 5)*	✓	✓	✓	✓	✓
25. Obtain written, informed consent from parents/guardians for collection, use, storage and destruction of children's personal information, including photos and videos.	✓	✓	✓		
26. Allow parents/guardians to withdraw consent for collection, storage and destruction of their child's personal information which includes photos and videos at any time.	✓	✓	✓		
27. Images or videos of children must not be shared on any public or personal social media accounts by staff, parents, or guardians.	✓	✓	✓	✓	✓
28. Create a shared understanding between EECS, families, early childhood teachers and educators about digital technology use, by adults, in front of children.	✓	✓	✓	✓	✓
29. Ensure safety procedures are developed and implemented for using ***digital communication platforms*** (refer to Definitions) with children and their families *(Appendix 2.25.05: Digital Communication Platform Safety Guidelines).*	✓	✓	✓		✓
30. Ensure when using digital documentation platforms, all staff consider the security of their digital data and the privacy of children and families *(refer to Policy 7.03 – Confidentiality and Privacy)*	✓	✓	✓		✓
31. Ensure that appropriate ***filtering*** and monitoring are in place for all devices used at the service	✓	✓	✓		✓
32. Consistently provide proactive supervision when young children are using digital technology, including ***smart toys*** *(refer to Policy 2.02: Supervision of Children).*	✓	✓	✓	✓	✓
33. Ensure effective supervision during digital play by arranging physical spaces so screens are always visible to staff. (*refer to Policy 2.02: Supervision of Children)*.		✓	✓		✓
34. Ensure screen-based activities are restricted to short, purposeful learning sessions integrated into the curriculum.		✓	✓		✓

Responsibilities	Approved Provider and EECS Unit	Nominated Supervisors/ Team Leaders	Early Childhood Teacher, Educators, and other staff	Family, parents/guardians	Contractors, volunteers, and students
35. Ensure children have what they need, can safely take part, and are protected when using ***digital technologies*** and online spaces.	✓	✓	✓		✓
36. Teach children about online safety, consent, privacy, and respectful technology use in ways appropriate to their age and development *(refer to Process 2.25.3: Teaching Digital and Online Safety)*.		✓	✓		✓
37. Respect children and family's diversity and strive to meet their needs for online safety education inclusive of gender, age, culture, ability, appearance, socioeconomic status, family background, geographical location, and access.	✓	✓	✓	✓	✓
38. Identify and document children's personal devices that are needed for communication or medical purposes (e.g. ***AAC device***, heart or blood sugar level monitoring) on *Appendix 2.26.06: Personal Electronic Device Authorised List.*	✓	✓	✓	✓	✓
39. Ensure processes are in place to ensure children and parents/guardian who speak languages other than English understand this policy.	✓	✓			
40. Make sure children know what to do if they see inappropriate content online.	✓	✓	✓		✓
41. Support the use of ***digital technologies*** in the curriculum as tools for designing, drawing, editing, reflecting and composing.		✓	✓		✓
42. Encourage the use of ***digital technologies*** in the curriculum for children to access images and information, explore diverse perspectives and make sense of their world.		✓	✓		✓
43. Ensure screen-based digital technology use while sitting is only for short periods and does not replace periods of active physical movement.		✓	✓		✓
44. Provide digital technology experiences for young children that promote movement opportunities.		✓	✓		✓
45. Support children to develop ***self-regulation*** when using digital technologies and support them to transition from digital to non-digital activities		✓	✓		✓
46. Model respectful and balanced technology use for children.		✓	✓	✓	✓
47. Provide families with information about online safety and risks in the online environment, such as ***online grooming***, ***cyber bullying*** and ***sexting***.	✓	✓	✓		✓
48. Share information with families on where to get help for online safety concerns, including external resources.	✓	✓	✓		
49. Guide families to reliable sources for advice on selecting suitable apps, games, and digital media for children. *(refer to Websites in Related Policies & Resources)*.	✓	✓	✓		
50. Support families to understand the effects of disturbing or arousing content and screen use before bedtime on children's sleep.	✓	✓	✓		

Responsibilities	Approved Provider and EECS Unit	Nominated Supervisors/ Team Leaders	Early Childhood Teacher, Educators, and other staff	Family, parents/guardians	Contractors, volunteers, and students
51. Develop ways for families to report negative online experiences, concerns, or incidents.	✓	✓			
52. Provide families with information on how to report an online incident or concern. *(refer to Policy 7.05: Complaints and Compliments).*	✓	✓			
53. Immediately report any suspected data breach or online safety incident/concern to a supervisor.	✓	✓	✓		✓
54. Promptly follow all procedures for recording and responding to data breaches or online safety incidents/concerns. *(Process 2.25.1: Reporting and Responding to Online Incident.)*	✓	✓	✓		✓
55. Ensure an online safety agreement is created in collaboration with children and families.	✓	✓	✓		

Definitions

The terms defined in this section relate specifically to this policy (*Definitions have been sourced from the Glossary section of the NQF Child Safe Culture and Online Safety Guides*):

AAC device: An Augmentative and Alternative Communication (AAC) device is a tool that helps people who have difficulty speaking or communicating. It can include things like communication boards, speech-generating devices, or apps that help a person express their thoughts, needs, or feelings.

Cyber bullying: When someone uses the internet to be mean to a child or young person, so they feel bad or upset.

Digital communication platforms: video teleconferencing software programs such as Zoom, Goggle Classroom, Microsoft Teams, Webex Meetings, Skype

Digital technologies: refers to electronic tools, systems, devices and resources that generate, store or process data. In the context of this policy, this includes (but is not limited to) computers, tablets, smart devices, interactive whiteboards, smart toys, cameras, audio-visual equipment, and internet-based platforms used for communication, learning, administration, and engagement with children, families, and staff.

Digital tool: Software, applications, or online platforms that are used to support learning, communication, organisation, or creativity through digital technology. These tools can help children and educators interact, share information, and complete tasks in online or digital environments.

Disclosure: A process by which a child conveys or attempts to convey that they are being or have been sexually abused, or by which an adult conveys or attempts to convey that they were sexually abused as a child. This may take many forms and might be verbal or non-verbal. Non-verbal disclosures using painting or drawing, gesticulating, or through behavioural changes, are more common among young children and children with cognitive or communication impairments. Children, in particular, may also seek to disclose sexual abuse through emotional or behavioural cues, such as heightened anxiety, withdrawal or aggression.

File transfer media: Any physical or digital device used to store, move, or share electronic files and data between computers or systems. This includes items such as USB drives, SD cards, external hard drives, CDs/DVDs, and digital platforms or services that allow file sharing or storage (e.g. cloud storage services like Google Drive or Dropbox).

Filtering: The use of digital tools or settings to restrict or block access to online content that is inappropriate, harmful, or not age-appropriate. Filtering helps protect users—particularly children—from exposure to unsafe or unsuitable material by preventing access to specific websites, applications, or online services based on predetermined criteria.

Harmful content: Harmful content includes:

- sexually explicit material
- false or misleading information
- violence
- extremism or terrorism
- hateful or offensive material.

Illegal content: Illegal content includes:

- images and videos of child sexual abuse
- content that advocates terrorist acts
- content that promotes, incites or instructs in crime or violence
- footage of real violence, cruelty and criminal activity.

LGBTQIA+: an acronym that stands for Lesbian, Gay, Bisexual, Transgender, Queer, Intersex, and Asexual. The “+” indicates the acronym also includes other sexual orientations and gender identities that are not explicitly listed. It is a broad term used to refer to a diverse community of people who experience same-sex or same-gender attraction, gender identities that differ from their assigned sex at birth, or other variations in sexual orientation and gender.

Online grooming: A form of child exploitation where an adult uses the internet or digital technologies to deliberately build a relationship with a child or young person, with the intent to manipulate, exploit, or abuse them. This may include gaining the child’s trust, isolating them from others, and encouraging them to share personal information, images, or engage in inappropriate behaviours.

Online hate: Any hateful posts about a person or group based on their race, religion, ethnicity, sexual orientation, disability or gender

Online platform: A website or digital space that allows people to connect, share, learn, or communicate over the internet. It often includes features like messaging, content sharing, or collaboration.

Personal storage devices: Electronic devices owned by an individual that are used to store or transfer digital data. These can include USB drives, external hard drives, SD cards, memory sticks, or any other portable media used to save files or information.

Self-regulation: The capacity for children (and adults) to regulate their behaviour in response to their emotions and thinking.

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.

Smart toys: Smart toys generally require an internet connection to operate as the computing task is on a central server.

Legislation and Standards

Relevant legislation and standards include but are not limited to:

- Education and Care Services National Law Act 2010
- Education and Care Services National Regulations 2011
- NQF Online Safety Guide (ACECQA, 2025)
- NQF Child Safe Culture Guide (ACECQA, 2025)
- National Quality Standard, Quality Area 2: Children Health and Safety and Quality & Area 7: Governance and Leadership
- Child Safe Standards
- Early Childhood Australia Code of Ethics
- Information Privacy Act 2000 (Vic)
- Occupational Health and Safety Act 2004 (Vic)
- Online Safety Act 2021
- Privacy Act 1988 (Cth)
- United Nations Convention on the Rights of the Child

Related Appendices & Documents

Appendix 2.25.1 – NQF Child Safe Culture Guide (ACECQA, 2025)
Appendix 2.25.2 – NQF Online Safety Guide (ACECQA, 2025)
Appendix 2.25.3 - Online Safety Incident Report Form
Appendix 2.25.4 - Online Safety Self-Assessment and Risk Assessment Tool
Appendix 2.25.5 – Digital Communication Platform Safety Guidelines
Appendix 2.25.6 – Personal Electronic Device Authorised List
Appendix 2.25.7 – Wyndham Records & Information Management Policy
Appendix 2.25.8 – Application Form: Use of Personal Device
Appendix 4.01.1 – WCC Corporate Code of Conduct
Appendix 4.01.2 – WCC Values and Behaviours
Process 2.25.1 - Reporting and responding to an online incident or concern
Process 2.25.2 – Photo and Video consent for children under 5
Process 2.25.3 – Teaching Digital and Online Safety in Early Education
Process 2.25.4 – Apply for Approval to Use Personal Device

Related Policies & Resources

2.01 – Providing a Child Safe Environment
2.02 – Supervision of Children
4.01 – Code of Conduct
7.03 – Confidentiality and Privacy

Resources:

Website – eSafety Early Years professional learning modules: https://www.esafety.gov.au/educators/training-for-professionals/early-years

Website – Early Childhood Australia Statement on young children and digital technology: http://www.earlychildhoodaustralia.org.au/wp-content/uploads/2018/10/Digital-policy-statement.pdf

Website – eSafety Commissioner: https://www.esafety.gov.au/

Website – National Model Code - Taking images in early childhood education and care: https://www.acecqa.gov.au/national-model-code-taking-images-early-childhood-education-and-care

Website – The eSafety Guide: https://www.esafety.gov.au/key-issues/esafety-guide

Website – The Playing IT Safe Framework and Alignment: https://playingitsafe.org.au/

Authorisation and Version Control

Version	Objective ID	Action	Date	Endorsement date	Next Review Date
1	A4702970	Newly developed policy ensuring compliance with Child Safe Standards.	23/01/2025	January 2025	January 2026
2	A4891264	Responsibilities, Appendices and resources reviewed and updated to reflect legislative changes coming into effect 1 September 2026 and alignment with the National Model Code	13/08/2025	22/08/2025 TPapaioannou	August 2026