

SAFE USE OF DIGITAL TECHNOLOGIES AND ONLINE ENVIRONMENTS

QUALITY AREA 2 & 7 | ELAA version 2.3

This document is provided as a guiding framework and has been thoughtfully adapted to reflect the values, philosophy, and community context of Ferguson Park Pre-School. Our service is committed to fostering a welcoming, inclusive, and play-based learning environment that respects the diverse cultural backgrounds, identities, and experiences of all children and families within our local community. While every effort has been made to ensure the information contained within this policy is accurate and relevant at the time of review, Ferguson Park Pre-School acknowledges that legislation, regulations, and best practice standards are subject to change. It is the responsibility of the Approved Provider and leadership team to regularly review and update all policies to maintain compliance and alignment with current requirements, as well as with the evolving needs of our children, families, and community.



Working in partnership with Cancer Council Victoria, ELAA has aligned this policy to the key policies and guidelines of the Healthy Early Childhood Services Achievement Program



PURPOSE

This policy will provide guidelines to ensure that all users of digital technologies at Ferguson Park Pre-School or on behalf of Ferguson Park Pre-School:

- Understand and follow procedures to ensure the safe and appropriate use of digital technologies Ferguson Park Pre-School, including maintaining secure storage of information
- take responsibility to protect and maintain privacy in accordance with the service's *Privacy and Confidentiality Policy*
- promote a child safe culture when it comes to taking, use, storage and destruction of images or videos of children
- are aware that only those persons authorised by the approved provider are permitted to access digital devices at the service
- understand what constitutes illegal and inappropriate use of digital devices and avoid such activities.
- understand and follow professional use of interactive digital technologies platforms, such as social media (*refer to Definitions*) and other information sharing platforms (*refer to Definitions*).



POLICY STATEMENT

The safety, health, wellbeing, rights and best interests of every child are the paramount consideration and must guide all decisions, actions and practices of educators within the education and care service.

VALUES

Ferguson Park Pre-School is committed to:

- providing 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
- professional, ethical and responsible use of digital technologies at the service
- providing a safe workplace for management, educators, staff and others using the service's digital technologies and information sharing platforms
- the rights of all children to feel safe, and be safe at all times



- safeguarding the privacy and confidentiality of information received, transmitted or stored electronically
- ensuring that the use of the service's digital technologies complies with all service policies and relevant government legislation
- providing management, educators and staff with online information, resources and communication tools to support the effective operation of the service.

SCOPE

This policy applies to the approved provider or persons with management or control, nominated supervisor, persons in day-to-day charge, early childhood teachers, educators, staff, students, volunteers, at Ferguson Park Pre-School. **This policy does not apply to children.** Where services are using digital technologies within their educational programs, they should develop a separate policy concerning the use of digital technologies by children (*refer to eSafety Policy*).

This policy applies to all aspects of the use of digital technologies including:

- desktop top computers, laptops/notebooks, tablets, iPads, smartphones and smart devices (including watches)
- copying, saving or distributing files
- electronic mail (email)
- file sharing
- file storage (including the use of end point data storage devices – *refer to Definitions*)
- file transfer/Cloud
- instant messaging
- internet usage
- portable communication devices including mobile and cordless phones.
- printing material
- social media (*refer to Definitions*)
- streaming media
- subscriptions to list servers, mailing lists or other like services
- video conferencing
- weblogs (blogs)

RESPONSIBILITIES	Approved provider and persons with management or control	Nominated supervisor and persons in day-to-day charge	Early childhood teacher, educators and all other staff	Parents/guardians	Contractors, volunteers and students
	R indicates legislation requirement, and should not be deleted				
1. Ensuring that the use of the service’s digital technologies complies with all relevant state and federal legislation (refer to Legislation and standards), and all service policies (including Privacy and Confidentiality Policy, eSafety for Children and Code of Conduct Policy) (Child Safe Standards 2-.2.3, 2.4, 2.6)	R	✓	✓	✓	✓



2. Ensuring staff understand how to actively supervise children while using digital technologies (<i>Child Safe Standards 8 – 8.1, 9 – 9.1</i>)	R	R			
3. Undertaking risk assessments (<i>refer to Sources</i>) identifying the service's digital technologies practices, identify strengths and areas for improvement (<i>Child Safe Standards 2- .2.5, 9 – 9.3</i>)	R	√	√		√
4. Obtaining parent/guardian consent before taking, retaining, or sharing images and videos of children (<i>refer to Enrolment and Orientation and Privacy and Confidentiality policy</i>) (<i>Child Safe Standards 4 – 4.2, 9 – 9.2</i>)	R	√	√		√
5. Asking children for permission before taking photos or videos and explain how these will be used (<i>Child Safe Standards 3 – 3.1</i>)	√	√	√		√
6. Regularly monitoring use of service-issued electronic devices to ensure that they are being used appropriately (<i>Child Safe Standards 2- 2.5, 9 – 9.2</i>)	R	√			
7. Ensuring capturing, using, storing, and disposing of images, videos, and audio recordings of children are in line with privacy requirements (<i>refer to Privacy and Confidentiality policy</i>) (<i>Child Safe Standards 2- 2.6, 9 – 9.2</i>)	R	√	√		√
8. Ensuring oversight and control of who has access to images (digital and hard copy) of children, including the movement of these onto devices and platforms (<i>Child Safe Standards 2- 2.6, 9 – 9.2</i>)	R	R			
9. Ensuring staff do not transfer images of children to their own account or device either directly or via the cloud, for example, to post images or videos on social media or other applications / software platforms that were not its intended purpose (<i>Child Safe Standards 2- 2.6, 9 – 9.2</i>)	R	R			
10. N/A no devices at this service. Ensuring surveillance and monitoring devices are in line with privacy requirements (<i>refer to CCTV policy</i>)	R	√			
11. Ensuring that the <i>Safe Use of Digital Technologies and Online Environments Policy</i> 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 (<i>Child Safe Standards 2- 2.5, 9 – 9.1</i>)	R	R	√		√
12. Promoting 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) (<i>Child Safe Standards 2- 2.2, 9 – 9.1, 9.2</i>)	R	√	√		√
13. Ensuring the safe use of digital technologies, including wearable devices, networks, platforms, apps, and networked toys within the service, and that they are password protected and in line with privacy principle (<i>refer to Privacy and Confidentiality policy</i>) (<i>Child Safe Standards 2- 2.6, 9 – 9.2</i>)	R	R	√		√
14. Ensuring that person who is providing education and care and working directly with children (<i>refer to Definitions</i>) do not	R	√	√	√	√



carry their personal electronic devices (<i>refer to Definitions</i>) while providing education and care to children, except for authorised essential purposes (<i>refer to Definitions</i>) (<i>Child Safe Standards 9 – 9.2</i>)					
15. Ensuring authorisation is documented for when a person who is providing education and care and working directly with children (<i>refer to Definitions</i>) may need to continue to carry their personal electronic device (<i>refer to Definitions</i>) while educating and care for children (example: medical conditions) (<i>Refer to Attachment 6</i>) (<i>Child Safe Standards 2- 2.6, 9 – 9.2</i>)	R	√			
16. Ensuring a suitable log is maintained to record all essential purpose authorisations forms, that all logs are stored securely and available at the service for authorised officers to inspect (<i>Child Safe Standards 2- 2.6</i>)	R	√			
17. Maintaining a log for third party professionals attending the service and working directly with children (such as an allied health or inclusion professional) that they are using business or organisation issued devices are used only for work purposes (and not personal use) (<i>Child Safe Standards 2- 2.6, 9 – 9.2, 9.4</i>)	R	R	√		√
18. Providing a secure place for persons who are providing education and care, and working directly with children (<i>refer to Definitions</i>), to store their personal digital devices while they are working with children	√	√			
19. Ensuring teachers and educators do not use personal devices for multi-factor authentication to access and use Arrival while providing education and care and working directly with children (<i>Child Safe Standards 2- 2.6, 9 – 9.2</i>)	R	R	R		R
20. Ensuring that personal devices are only accessed by teachers, educators and other staff when they are not providing education and care or working directly with children. Examples could include: - while taking a scheduled break from work, such as a lunch or tea break - during planning time - during administrative activities. Staff can also carry and use personal electronic devices that: - cannot take images or videos, and - are not storage and file transfer media (<i>Child Safe Standards 9 – 9.2</i>)	R	R	R		R
21. Undertaking risk assessments identifying whether personal devices (including wearable devices) can be used at the service and in what circumstances (<i>Child Safe Standards 2- 2.5, 9 – 9.2</i>)	R	R	√		√
22. Managing inappropriate use of digital technologies as described in <i>Attachment 2</i> (<i>Child Safe Standards 2- 2.4, 7 – 7.3, 9 – 9.2</i>)	R	√			
23. Providing suitable digital technologies facilities to enable early childhood teachers, educators and staff to effectively manage and operate the service (<i>Child Safe Standards 2- 2.5, 9 – 9.2</i>)	R	√			



24. Ensuring there are sufficient service-issued devices available when programs are delivered outside the approved service premises (such as bush, beach or other nature programs) (<i>Child Safe Standards 9 – 9.3</i>)	R	R			
25. Ensuring that personal devices that take and store images are only used for emergency during excursions and regular outings, and that essential purposes authorisation (<i>refer to Attachment 6</i>) documentation is completed prior to excursions and regular outings (<i>Child Safe Standards 2- 2.6, 9 – 9.2</i>)	R	R	√	√	√
26. Ensuring restricted persons (<i>refer to Definitions</i>) do not use their personal devices to record images of children when providing education and care and working directly with children (<i>Child Safe Standards 9 – 9.2</i>)	R	√	√	√	√
27. Ensuring parents/guardians do not use their personal devices to record images of children, this includes during service events (<i>Child Safe Standards 4 – 4.2, 9 – 9.2</i>)	R			√	
28. Ensuring third party professional attending the service and working directly with children (such as an allied health or inclusion professional) only use devices that are issued by their business or institution; and is used only for work purposes (and not personal use) (<i>Child Safe Standards 9 – 9.2, 9.4</i>)	R	√	√		√
29. Authorising the access of early childhood teachers, educators, staff, volunteers and students to the service's digital technologies facilities, as appropriate (<i>Child Safe Standards 2- 2.6, 9 – 9.2</i>)	R	R			
30. Providing clear procedures and protocols that outline the parameters for use of the service's digital technologies facilities both at the service and when working from home (<i>refer to Attachment 1</i>) (<i>Child Safe Standards 2- 2.6, 9 – 9.2</i>)	√	√			
31. Avoiding inappropriate conduct (<i>Refer to Definitions</i>) and at all times, maintaining professional boundaries, and act in line with the <i>Code of Conduct, Child Safe Environment and Wellbeing Policy and Interaction with children</i> (<i>Child Safe Standards 2- 2.6</i>)	R	R	R		R
32. Embedding a culture of awareness and understanding of security issues at the service (<i>Child Safe Standards 2- 2.2</i>)	R	√	√	√	√
33. Never posting online photos or videos of children who: - Are known to child protection, family court, or criminal proceedings - Are experiencing family violence or need to remain anonymous - Have parents concerned about their child's digital footprint (<i>Child Safe Standards 2 – 2.3, 5 – 5.1</i>)	R	√	√		√
34. Ensuring that effective financial procedures and security measures are implemented where transactions are made using the service's digital technologies facilities, e.g. handling fees, invoice payments, and using online banking	R	√			



35. Ensuring that the service's computer software and hardware are purchased from an appropriate and reputable supplier (<i>Child Safe Standards 9 – 9.4</i>)	√	√			
36. Identifying the need for additional password-protected email accounts for management, early childhood teachers, educators, staff and others at the service, and providing these as appropriate (<i>Child Safe Standards 2- 2.5</i>)	√	√			
37. Removing access on online platforms for staff, parents/guardians and others when they leave the service (<i>Child Safe Standards 2- 2.5</i>)	R	R			
38. Identifying the training needs of early childhood teachers, educators and staff in relation to digital technologies, and providing recommendations for the inclusion of training in digital technologies in professional development activities (<i>Child Safe Standards 8 – 8.2</i>)	√	√			
39. Ensuring regular backup of critical data and information at the service (<i>refer to Attachment 1</i>) (<i>Child Safe Standards 2- 2.5</i>)	√	√	√		
40. Ensuring secure storage of all information (including images and videos of children) at the service, including backup files (<i>refer to Privacy and Confidentiality Policy</i>) (<i>Child Safe Standards 2- 2.5</i>)	R	√	√		
41. Adhering to the requirements of the <i>Privacy and Confidentiality Policy</i> in relation to accessing information on the service's computer/s, including emails (<i>Child Safe Standards 2- 2.6</i>)	R	R	R		
42. Considering encryption (<i>refer to Definitions</i>) of data for extra security (<i>Child Safe Standards 2- 2.5</i>)	√	√			
43. Ensuring that reputable anti-virus and firewall software (<i>refer to Definitions</i>) are installed on service computers, and that software is kept up to date (<i>Child Safe Standards 2- 2.5</i>)	√	√			
44. Developing procedures to minimise unauthorised access, use and disclosure of information and data, which may include limiting access, passwords, multifactor authentication and encryption (<i>refer to Definitions</i>) (<i>Child Safe Standards 2- 2.5</i>)	R	√			
45. Ensuring that the service's liability in the event of security breaches, or unauthorised access, use and disclosure of information and data is limited by developing and publishing appropriate disclaimers (<i>refer to Definitions</i>) (<i>Child Safe Standards 2- 2.5</i>)	R	√			
46. Developing procedures to ensure data and information (e.g. passwords) are kept secure, and only disclosed to individuals where necessary e.g. to new educators, staff or committee of management (<i>Child Safe Standards 2- 2.5</i>)	R	√			
47. Being aware of the requirements and complying with this policy (<i>Child Safe Standards 2- 2.2, 2.6</i>)	√	√	√	√	√
48. Appropriate use of endpoint data storage devices (<i>refer to Definitions</i>) by digital technologies users at the service (<i>Child Safe Standards 2- 2.5</i>)	R	√	√	√	√



49. Ensuring that all material stored (including images and videos of children) on endpoint data storage devices is also stored on a backup drive, and that both device and drive are kept in a secure location (<i>Child Safe Standards 2- 2.5</i>)	R	✓	✓		✓
50. Ensuring that written permission is provided by parents/guardians for authorised access to the service's computer systems and internet by persons under 18 years of age (e.g. a student on placement at the service) (<i>refer to Attachment 5</i>). (<i>Child Safe Standards 2- 2.6, 4 – 4.2</i>)	R	✓			✓
51. Developing guidelines on the use of Artificial Intelligence (AI) (<i>refer to Attachment 7</i> (if applicable to the service) (<i>Child Safe Standards 2- 2.5</i>)	✓	✓			
52. Providing authorisation to early childhood teachers, educators and staff to be social media representatives for Ferguson Park Pre-School (<i>refer to Attachment 3</i>) (<i>Child Safe Standards 2- 2.3</i>)	✓	✓			
53. Complying with all relevant legislation and service policies, protocols and procedures, including those outlined in <i>Attachments 1</i> (<i>Child Safe Standards 2- 2.3</i>)	R	R	R	R	R
54. Reading and understanding what constitutes inappropriate use of digital technologies (<i>refer to Attachment 2</i>) (<i>Child Safe Standards 2- 2.4, 2.5, 8 – 8.2</i>)	✓	✓	✓	✓	✓
55. Ensuring that if working from home, the service device does not leave the service unless they contain no images of children (<i>refer to Attachment 1 and 4</i>) (<i>Child Safe Standards 2- 2.5</i>)	R	R	✓		✓
56. Completing the authorised user agreement form when using service devices outside the service. The device must be password protected (<i>refer to Attachment 4</i>) (<i>Child Safe Standards 2- 2.5</i>)	✓	✓	✓		✓
57. Maintaining the security of digital technologies facilities belonging to Ferguson Park Pre-School and keeping allocated passwords secure, including not sharing passwords and logging off after using a computer (<i>Child Safe Standards 2- 2.5</i>)	R	R	R	✓	R
58. Accessing accounts, data or files on the service's computers only where authorisation has been provided (<i>Child Safe Standards 2- 2.5</i>)		✓	✓		✓
59. Co-operating with other users of the service's digital technologies to ensure fair and equitable access to resources	✓	✓	✓		✓
60. Obtaining approval from the approved provider before purchasing licensed computer software and hardware (<i>Child Safe Standards 2- 2.5</i>)		✓	✓		
61. Ensuring no illegal material is transmitted at any time via any digital technology medium (<i>refer to Attachment 2</i>) (<i>Child Safe Standards 2- 2.4, 9 – 9.2</i>)	R	✓	✓	✓	✓
62. Using the service's email, messaging and social media (<i>refer to Definitions</i>) facilities for service-related and lawful activities only (<i>refer to Attachment 2</i>) (<i>Child Safe Standards 2- 2.4, 9 – 9.2</i>)	✓	✓	✓	✓	✓



63. Using endpoint data storage devices (<i>refer to Definitions</i>) supplied by the service for service-related business only, and ensuring that this information is protected from unauthorised access and use (<i>Child Safe Standards 2- 2.4, 9 – 9.2</i>)		✓	✓		✓
64. Notifying the approved provider of any damage, faults or loss of endpoint data storage devices (<i>Child Safe Standards 2- 2.6</i>)		R	R		R
65. Notifying the approved provider and/or nominated supervisor immediately if they observe any inappropriate use of personal or service issued electronic devices at the service (<i>Child Safe Standards 2- 2.6</i>)			✓	✓	✓
66. Signing an acknowledgement form upon receipt of a USB or portable storage device (including a laptop) (<i>refer to Attachment 4</i>) (<i>Child Safe Standards 2- 2.6</i>)		✓	✓		✓
67. Restricting the use of personal mobile phones to rostered breaks, and only used in areas outside of spaces being utilised for education and care of children (<i>Child Safe Standards 9 – 9.2</i>)	✓	✓	✓	✓	✓
68. Responding only to emergency phone calls when responsible for supervising children to ensure adequate supervision of children at all times (<i>refer to Supervision of Children Policy</i>) (<i>Child Safe Standards 2- 2.5</i>)	✓	✓	✓		✓
69. Ensuring electronic devices and files containing images and information about children and families are kept secure at all times (<i>refer to Privacy and Confidentiality Policy</i>) (<i>Child Safe Standards 2- 2.5</i>)	R	R	R		R
70. Responding to a privacy breach in accordance with <i>Privacy and Confidentiality policy</i> (<i>Child Safe Standards 2- 2.6</i>)	R	✓			
71. Complying with the appropriate use of social media (<i>refer to Definitions</i>) platforms (<i>refer to Attachment 3</i>) (<i>Child Safe Standards 2- 2.4</i>)	✓	✓	✓		✓
72. Complying with this policy at all times to protect the privacy, confidentiality and interests of Ferguson Park Pre-School employees, children and families (<i>Child Safe Standards 2- 2.6, 9 – 9.2</i>)	R	R	R		R



PROCEDURES

Refer to *Attachment 1* for the following procedures

- Email usage
- Digital storage of personal and health information
- Data back up
- Password management



BACKGROUND AND LEGISLATION



BACKGROUND

The digital technology landscape is constantly evolving, with early childhood services increasingly using fixed, wireless, and mobile devices to support research, communication, and service management. While these technologies offer cost-effective and efficient tools, they also come with significant legal and ethical responsibilities regarding information privacy, security, and the protection of employees, families, and children.

Approved providers and their staff must remain informed about emerging technologies and proactively manage associated risks, including exposure to harmful content, cyberbullying, and risks amplified by Artificial Intelligence (AI) tools. For example, digital toys connected to apps on phones or tablets can create cybersecurity vulnerabilities, enabling hackers to access Wi-Fi networks, track device locations, and potentially use audio and video functions, posing serious safety risks for children.

State and federal legislation covering information privacy, copyright, occupational health and safety, anti-discrimination, and sexual harassment applies to the use of digital technologies. Inappropriate or unlawful use includes accessing pornography, engaging in fraud, defamation, copyright infringement, unlawful discrimination or vilification, harassment (including sexual harassment, stalking, and privacy breaches), and illegal activities such as peer-to-peer file sharing. Continuous improvement in online safety practices is essential to safeguard all members of the service community.

The Victorian Government funds the State Library Victoria to provide IT support to kindergarten Early Years Management organization and community-based kindergarten services that operate funded kindergarten programs.

Through the Kindergarten IT Program, the State Library Victoria provides the following services to eligible organisations:

- Internet connectivity for kindergartens (data connection only)
- Twenty email addresses per kindergarten
- User support for general computer and Microsoft software enquiries
- Web hosting options
- Coordinated IT Training for eligible services including privacy and cyber safety training
- Providing advice for kindergartens purchasing new computers with the option to supply and install (kindergartens meet the purchase and installation costs)
- Repair of computer hardware that was provided by the Department of Education through the Kindergarten IT Project roll-out

The Victorian Regulatory Authority requires approved providers to comply with the National Model Code. The National Model Code is crucial for Early Childhood Education and Care (ECEC) services to ensure the safety and privacy of children. Under the Code, only service-issued electronic devices should be used for taking photos or recording videos, thereby minimising the risk of unauthorised distribution of images. The Code states that clear guidelines are developed on carrying personal devices for specific essential purposes ensuring that any exceptions are justified and controlled. Additionally, implementing strict controls for storing and retaining images or recordings of children is vital to protect their privacy and prevent misuse of sensitive information. Adhering to these guidelines not only safeguards children but also fosters trust and transparency between ECEC services and families.

LEGISLATION AND STANDARDS

Relevant legislation and standards include but are not limited to:

- Broadcasting Services Act 1992 (Cth)
- Charter of Human Rights and Responsibilities Act 2006 (Vic)
- Crimes Act 1958 (Vic)
- Classification (Publications, Films and Computer Games) Act 1995
- Commonwealth Classification (Publication, Films and Computer Games) Act 1995
- Competition and Consumer Act 2010 (Cth)
- Copyright Act 1968 (Cth)



- Copyright Amendment Act 2006 (Cth)
- Cybercrime Act 2001 (Cth)
- Education and Care Services National Law Act 2010
- Education and Care Services National Regulations 2011
- Equal Opportunity Act 2010 (Vic)
- Freedom of Information Act 1982
- Health Records Act 2001 (Vic)
- Information Privacy Act 2000 (Vic)
- National Quality Standard, Quality Area 7: Governance and Leadership
- Occupational Health and Safety Act 2004 (Vic)
- Privacy Act 1988 (Cth)
- Privacy and Data Protection Act 2014 (Vic)
- Protected Disclosure Act 2012 (Vic)
- Public Records Act 1973 (Vic)
- Sex Discrimination Act 1984 (Cth)
- Spam Act 2003 (Cth)
- Trade Marks Act 1995 (Cth)

The most current amendments to listed legislation can be found at:

Victorian Legislation – Victorian Law Today: www.legislation.vic.gov.au

Commonwealth Legislation – Federal Register of Legislation: www.legislation.gov.au



DEFINITIONS

The terms defined in this section relate specifically to this policy. For regularly used terms e.g. Approved Provider, Nominated Supervisor, Notifiable Complaints, Serious Incidents, Duty of Care, etc. refer to the Definitions file of the PolicyWorks catalogue.

Anti-spyware: Software designed to remove spyware: a type of malware (*refer to Definitions*), that collects information about users without their knowledge.

Artificial intelligence (AI): An engineered system that generates predictive outputs such as content, forecasts, recommendations, or decisions for a given set of human defined objectives or parameters without explicit programming. AI systems are designed to operate with varying levels of automation.

AI Tools: Software, platforms, devices, or apps powered by AI, including chatbots, voice assistants, content-sorting algorithms, and AI-enabled toys or applications.

Chain email: An email instructing recipients to send out multiple copies of the same email so that circulation increases exponentially.

Computer virus: Malicious software programs, a form of malware (*refer to Definitions*), that can spread from one computer to another through the sharing of infected files, and that may harm a computer system's data or performance.

Cyber safety: The safe and responsible use of technology including use of the internet, electronic media and social media in order to ensure information security and personal safety. There are three main areas of risk to safety:

- Content: being exposed to illegal, inappropriate or harmful material
- Contact: being subjected to harmful online interactions with other users (including bullying)
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm.

Defamation: To injure or harm another person's reputation without good reason or justification. Defamation is often in the form of slander or libel.



Disclaimer: Statement(s) that seeks to exclude or limit liability and is usually related to issues such as copyright, accuracy and privacy.

Electronic communications: Email, instant messaging, communication through social media and any other material or communication sent electronically.

Encryption: The process of systematically encoding data before transmission so that an unauthorised party cannot decipher it. There are different levels of encryption available.

Endpoint data storage devices: Devices capable of storing information/data. New devices are continually being developed, and current devices include:

- laptops
- USB sticks, external or removable hard drives, thumb drives, pen drives and flash drives
- iPods or other similar devices
- cameras with USB drive connection
- iPhones/smartphones
- PCI/PC Card/PCMCIA storage cards
- PDAs (Personal Digital Assistants)
- other data-storage devices (CD-ROM and DVD).

Essential purposes: The use and / or possession of a personal electronic device may be authorised for purposes other than taking images or recording videos of children include:

- communication in an emergency situation involving a lost child, injury to child or staff member, or other serious incident, or in the case of a lockdown or evacuation of the service premises
- personal health requirements, e.g. heart or blood sugar level monitoring
- disability, e.g. where a personal electronic device is an essential means of communication for an educator or other staff member
- family necessity, e.g. a worker with an ill or dying family member
- technology failure, e.g. when a temporary outage of service-issued electronic devices has occurred
- local emergency event occurring, to receive emergency notifications through government warning systems, for example, bushfire evacuation text notification.

Firewall: The primary method of keeping a computer/network secure. A firewall controls (by permitting or restricting) traffic into and out of a computer/network and, as a result, can protect these from damage by unauthorised users.

Flash drive: A small data-storage device that uses flash memory, and has a built-in USB connection. Flash drives have many names, including jump drives, thumb drives, pen drives and USB keychain drives.

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.

Information sharing platforms: Describes the exchange of data between various organisations, people and technologies This can include but no limited to Dropbox, Google Drive, Sharepoint, Skype for Business, One Drive

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.

Inappropriate conduct: Conduct that a reasonable person would consider inappropriate in an education and care service, taking into account any of the following circumstances:

- Whether the conduct aligns with generally accepted education and care practice



- The child's age and developmental stage
- Whether the conduct is likely to cause or result in harm (including emotional, psychological or physical harm) or injury to a child or children
- Whether the conduct is sexual, aggressive or violent.

In deciding if the conduct is inappropriate, it does not matter if:

- the child consented (agreed to the conduct, either by directly expressing their consent or implying consent through their actions)
- the person subjecting the child to the conduct believes the child has consented
- the person subjecting the child to the conduct is related to the child.

Subjecting a child to inappropriate conduct can occur in a number of ways including, but not limited to:

- in-person via words or behaviour, including both adult to child or between adults in the presence of a child/ren
- filming and capturing images or recordings
- as a single occasion or as part of a pattern over time
- either directly or indirectly (for example, exposure to inappropriate language or conversations, or leaving inappropriate material accessible to children)
- online
- as an omission (for example, deliberately excluding a child).

Integrity: (In relation to this policy) refers to the accuracy of data. Loss of data integrity may be either gross and evident (e.g. a computer disk failing) or subtle (e.g. the alteration of information in an electronic file).

Malware: Short for 'malicious software'. Malware is intended to damage or disable computers or computer systems.

PDA's (Personal Digital Assistants): A handheld computer for managing contacts, appointments and tasks. PDA's typically include a name and address database, calendar, to-do list and note taker. Wireless PDA's may also offer email and web browsing, and data can be synchronised between a PDA and a desktop computer via a USB or wireless connection.

Person who is providing education and care and working directly with children: In the context of this policy a person includes:

- teachers and educators, including casual and agency staff
- students attending the service as part of a practicum and representatives of tertiary providers who attend the service to assess students
- volunteers, including parent volunteers
- any third parties delivering programs or incursion activities to children in a service, whether paid or unpaid
- allied health and inclusion professionals attending a service to observe, assess or work with a child at the service
- mentors or coaches attending the service to support teachers or educators working with children or providing education and care
- preschool field officers
- primary school teachers attending a service as part of a school transition program.

If a third party professional attending a service and working directly with children (such as an allied health or inclusion professional) needs to use a device (for example, to undertake an assessment or take notes) they can use a device that is:

- issued by their business or institution; and
- used only for work purposes (and not personal use).

Personal Electronic Device: A device that can take photos, record or store videos refers to any handheld or portable device owned by an individual, such as a smartphone, smart watches with camera/recording functionality, tablet, or digital camera, personal storage and file transfer media

(such as



SD cards, digital cameras, wearables, such as camera glasses, USB drives, hard drives and cloud storage), which has the capability to capture and store images or video footage. These devices are not issued or controlled by the approved provider.

Phishing: Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.

Portable storage device (PSD) or removable storage device (RSD): Small, lightweight, portable easy-to-use device that is capable of storing and transferring large volumes of data. These devices are either exclusively used for data storage (for example, USB keys) or are capable of multiple other functions (such as iPods and PDAs).

Ransomware: Ransomware is a type of malicious software that threatens to publish the victim's data or block access to it unless a ransom is paid.

Restricted persons: The National Model Code restrictions apply to any person who is providing education and care and working directly with children include:

- teachers and educators, including casual and agency staff
- students attending the service as part of a practicum and representatives of tertiary providers who attend the service to assess students
- volunteers, including parent volunteers
- any third parties delivering programs or incursion activities to children in a service, whether paid or unpaid
- allied health and inclusion professionals attending a service to observe, assess or work with a child at the service
- mentors or coaches attending the service to support teachers or educators working with children or providing education and care
- preschool field officers
- primary school teachers attending a service as part of a school transition program.

If a third party professional attending a service and working directly with children (such as an allied health or inclusion professional) needs to use a device (for example, to undertake an assessment or take notes) they can use a device that is:

- issued by their business or organisation; and
- used only for work purposes (and not personal use).

Security: (In relation to this policy) refers to the protection of data against unauthorised access, ensuring confidentiality of information, integrity of data and the appropriate use of computer systems and other resources.

Social Media: A computer-based technology that facilitates the sharing of ideas, thoughts, information and photos through the building of virtual networks and communities. Examples can include but not limited to, Facebook, YouTube, WhatsApp, Facebook Messenger, TikTok and Instagram

Spam: Unsolicited and unwanted emails or other electronic communication.

USB interface: Universal Serial Bus (USB) is a widely used interface for attaching devices to a host computer. PCs and laptops have multiple USB ports that enable many devices to be connected without rebooting the computer or turning off the USB device.

USB key: Also known as sticks, drives, memory keys and flash drives, a USB key is a device that plugs into the computer's USB port and is small enough to hook onto a key ring. A USB key allows data to be easily downloaded and transported/transferred.

Virus: A program or programming code that multiplies by being copied to another program, computer or document. Viruses can be sent in attachments to an email or file, or be present on a disk or CD. While some viruses are benign or playful in intent, others can be quite harmful: erasing data or requiring the reformatting of hard drives.



Vishing: Vishing is a form of phishing that uses the phone system or voice over internet protocol (VoIP) technologies. The user may receive an email, a phone message, or even a text encouraging them to call a phone number due to some discrepancy. If they call, an automated recording prompts them to provide detailed information to verify their account such as credit card number, expiration date or birthdate.



SOURCES AND RELATED POLICIES

SOURCES

- Department of Education: [Acceptable Use Policy, DE Information, Communications and Technology \(ICT\) Resources](#)
- IT for Kindergartens: www.kindergarten.vic.gov.au
- ACECQA: [National Model Code - Taking images in early childhood education and care](#)
- ACECQA: [Empowering children under 5 by asking them to give consent for photos or videos](#)
- ACECQA: [NQF Online Safety Guide Self and Risk Assessment Tool](#)
- ACECQA: [Consent and children's rights](#)
- ACECQA: [How do I manage a data breach?](#)
- OAIC: [Guidance on privacy and the use of commercially available AI products](#)

RELATED POLICIES

- CCTV
- Child Safe Environment and Wellbeing
- Code of Conduct
- Compliments and Complaints
- Educational Program
- Enrolment and Orientation
- eSafety for Children
- Excursions, Regular Outings and Service Events
- Governance and Management of the Service
- In nature programs
- Occupational Health and Safety
- Privacy and Confidentiality
- Staffing



EVALUATION

In order to assess whether the values and purposes of the policy have been achieved, the Approved Provider will:

- regularly seek feedback from everyone affected by the policy regarding its effectiveness
- monitor the implementation, compliance, complaints and incidents in relation to this policy
- keep the policy up to date with current legislation, research, policy and best practice
- revise the policy and procedures as part of the service's policy review cycle, or as required
- notifying all stakeholders affected by this policy at least 14 days before making any significant changes to this policy or its procedures, unless a lesser period is necessary due to risk ([Regulation 172 \(2\)](#))



ATTACHMENTS

- Attachment 1: Procedures for use of digital technologies at the service
- Attachment 2: Unacceptable/inappropriate use of digital technologies



- Attachment 3: Social Media Guidelines
- Attachment 4: Authorised user agreement
- Attachment 5: Parent/guardian authorisation for under-age access to the Ferguson Park Pre-School digital technology facilities:
- Attachment 6: Essential purpose authorisations
- Attachment 7: Guidelines for the use of AI
- Attachment 8: Storypark Consent
- Attachment 9: Ferguson Park Pre-School Educational Philosophy 2026
- Attachment 10: eSafety checklist for early learning services
- Attachment 11: NQF Child Safe Culture Self-assessment and risk assessment tool



AUTHORISATION

This policy was adopted by the approved provider of Ferguson Park Pre-School on **14/5/2014**.

Revised and reviewed on **16/07/2016, 16/05/2017, 16/04/2018, 30/08/2019, 01/03/2021, 16/06/2022, 04/09/2023, 17/01/2024, 05/08/2024, 05/09/2025, 12/05/2026**.

REVIEW DATE: 12/05/2027.



ATTACHMENT 1. PROCEDURES FOR USE OF DIGITAL TECHNOLOGIES AT THE SERVICE

Email usage

- Content of emails and email addresses must always be checked before sending.
- When sending emails to multiple recipients, care should be taken to avoid the inappropriate disclosure of email addresses to a whole group of recipients; blind copying (BCC) should be used where appropriate.
- Always include a subject description in the subject line.
- Create an email signature that identifies employee name, title, service name, service phone number and address
- Always include a disclaimer (*refer to Definitions*) which is common to all users, on emails to limit liability.
- Be cautious about opening files or launching programs that have been received as an attachment via email from the email itself. Instead, save an attachment to disk and scan with anti-virus software before opening, and keep an eye out for unusual filenames.
- Never open emails if unsure of the sender.
- Check email accounts on a regular basis and forward relevant emails to the approved provider or appropriate committee members/staff.
- Remove correspondence that is no longer required from the computer quarterly.
- Respond to emails as soon as is practicable.
- Never send unauthorised marketing content or solicitation emails
- Be suspicious of phishing titles.

Digital storage of personal and health information

- Digital records containing personal, sensitive and/or health information, or images of children must be password protected and stored securely so that privacy and confidentiality is maintained. This information must not be removed from the service without authorisation, as security of the information could be at risk (*refer to Privacy and Confidentiality Policy*).
- Digital records containing personal, sensitive and/or health information, or images of children may need to be removed from the service from time-to-time for various reasons, including for:
 - excursions and service events (*refer to Excursions and Service Events Policy*)
 - offsite storage, where there is not enough space at the service premises to store the records.

In such circumstances, services must ensure that the information is transported, handled and stored securely so that privacy and confidentiality is maintained at all times.

- Digital technology users are not to view or interfere with other users' files or directories, knowingly obtain unauthorised access to information or damage, delete, insert or otherwise alter data without permission.
- Ensure all material stored on an endpoint data storage device is also stored on a backup drive, and that both device and drive are kept in a secure location.

Backing up data

Data backup is the process of creating accessible data copies for use in the event of breach or loss.

- Develop a written backup plan that identifies:
 - What's being backed up
 - Where it's being backed up
 - How often backups will occur
 - Who's in charge of performing backups
 - Who's in charge of monitoring the success of these backups
 - How will backup drives be stored securely

Services can choose to either between onsite or remote backup:

- Onsite Backup
 - copy data to a second hard drive, either manually or at specified intervals.
- Remote Backup- cloud based backup server
 - install the software on every computer containing data that needs to be backed up,
 - set up a backup schedule, and
 - identify the files and folders to be copied.



Password management

The effective management of passwords is the first line of defence in the electronic security of an organisation. Every ICT facility should have a password strategy in place as part of the overall security strategy. The technical considerations and principals outlined below are intended to be used as a guide for developing a password procedure.

Technical considerations include:

- a strong password should:
 - Be at least 8 characters in length
 - Contain both upper and lowercase alphabetic characters (e.g. A-Z, a-z)
 - Have at least one numerical character (e.g. 0-9)
 - Have at least one special character (e.g. ~!@#\$%^&*()_-=)
- always verify a user's identity before resetting a password
- change passwords when an employer leaves the service
- password rotation; changed every 90 days or less
- do not use automatic logon functionality
- use of account lockouts for incorrect passwords, with a limit of 5 or fewer bad attempts.

Users should always follow these principles:

- do not share passwords with anyone. If there is an issue that requires you to do so, remember to change the password immediately after the issue has been resolved.
- never use the same password for work accounts as the one you have for personal use (banking, etc.).
- do not write down passwords or include them in an email.
- do not store passwords electronically unless they are encrypted.
- never use the "remember password" feature on any systems; this option should be disabled
- Do not use the same password for multiple administrator accounts.

Working from home

When an approved provider, nominated supervisor, early childhood teachers, educators or staff members are working from home they must:

- complete the authorised user agreement form (*refer to Attachment 4*)
- that images of children are not accessed, or transferred onto personal devices
- conduct a workstation assessment; taking reasonable care in choosing a suitable work space, including ergonomics, lighting, thermal comfort, safety, and privacy
- ensure security and confidentiality of work space, keeping private, sensitive, health information, planning, educational programs and children's records confidential and secure at all times
- keep allocated passwords secure, including not sharing passwords and logging off after using a computer
- adhere to the *Privacy and Confidentiality Policy*
- report breaches to privacy or loss of private, sensitive, and health information to nominated superiors as soon as practically possible.



ATTACHMENT 2. UNACCEPTABLE/INAPPROPRIATE USE OF DIGITAL TECHNOLOGY FACILITIES

Users of the digital technologies facilities (and in particular, the internet, email and social media) provided by Ferguson Park Pre-School must not:

- create or exchange messages that are offensive, harassing, obscene or threatening
- create, copy, transmit or retransmit chain emails (*refer to Definitions*), spam (*refer to Definitions*) or other unauthorised mass communication
- use the digital technology facilities as a platform to gain unauthorised access to other systems
- carry out activities that are illegal, inappropriate or offensive to fellow employees or the public. Such activities include, but are not limited to, hate speech or material that ridicules/discriminates against others on the basis of race, nationality, creed, religion, ability/disability, gender or sexual orientation
- use the digital technology facilities to access, download, create, store or distribute illegal, offensive, obscene or objectionable material (including pornography and sexually explicit material). It will not be a defence to claim that the recipient was a consenting adult
- use the digital technology facilities to make any personal communication that could suggest that such communication was made in that person's official capacity as an employee or volunteer of Ferguson Park Pre-School
- conduct any outside business or engage in activities related to employment with another organisation
- play games
- use the facilities to assist any election campaign or lobby any government organisation
- exchange any confidential or sensitive information held by Ferguson Park Pre-School unless authorised as part of their duties
- publish the service's email address on a 'private' business card
- harass, slander, intimidate, embarrass, defame, vilify, seek to offend or make threats against another person or group of people
- breach copyright laws through making copies of, or transmitting, material or commercial software.

Breaches of this policy

- Individuals who use digital technologies at the service for unlawful purposes may be liable to criminal or civil legal action. This could result in serious consequences, such as a fine, damages and/or costs being awarded against the individual, or imprisonment. The approved provider will not defend or support any individual using the service's digital technology facilities for an unlawful purpose.
- The service may block access to internet sites where inappropriate use is identified.
- Employees who fail to adhere to this policy may be liable to counselling, disciplinary action or dismissal.
- Management, educators, staff, volunteers and students who fail to adhere to this policy may have their access to the service's digital technology facilities restricted/denied.

Category 1: illegal — criminal use of material

This category includes but is not limited to:

- child abuse material offences relating to child pornography covered by the Crimes Act 1958 (Vic). 'Child abuse material' is defined in section 51A of the Crimes Act 1958 (Vic)
- objectionable material — offences relating to the exhibition, sale and other illegal acts relating to 'objectionable films' and 'objectionable publications' covered by the Classification (Publications, Films and Computer Games) (Enforcement) Act 1995 (Vic). Such material has or would attract a classification of X18+ (restricted) or RC (refused classification) under the Guidelines for Classification of Films 2012, Guidelines for the Classification of Computer Games 2012 or National Classification Code scheduled to the Classification (Publications, Films and Computer Games) Act 1995 (Cth)
- reckless or deliberate copyright infringement and any other material or activity that involves or is in furtherance of a breach of criminal law

Category 2: extreme — non-criminal use of material

This category includes non-criminal use of material that has or may attract a classification of RC or X18+ under the Guidelines for Classification of Films 2012, Guidelines for the Classification of Computer Games 2012 or National Classification Code scheduled to the Classification (Publications, Films and Computer Games) Act 1995 (Cth).

This includes any material that:



- depicts, expresses or otherwise deals with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that the material should not be classified
- describes or depicts in a way that is likely to cause offence to a reasonable adult or a person who is, or appears to be, a child under 18 (whether or not the person is engaged in sexual activity or not)
- promotes, incites or instructs in matters of crime or violence
- includes sexually explicit material that contains real depictions of actual sexual intercourse and other sexual activity between consenting adults

Category 3: critical — offensive material

This category includes other types of restricted or offensive material, covering any material that:

- has or may attract a classification of R18+ under the Guidelines for Classification of Films 2012, Guidelines for the Classification of Computer Games 2012 or National Classification Code scheduled to the Classification (Publications, Films and Computer Games) Act 1995 (Cth). Material may contain sex scenes and drug use that are high in impact
- includes sexualised nudity
- involves racial or religious vilification
- is unlawfully discriminatory
- is defamatory
- involves sexual harassment or bullying

Category 4: serious

- This category includes any use which is offensive or otherwise improper.
- The categories do not cover all possible breaches of this policy. Matters not covered by the above categories will be dealt with on an individual basis and on the relevant facts.



ATTACHMENT 3. SOCIAL MEDIA AND INFORMATION SHARING PLATFORM GUIDELINES

The below directives are essential to the safety and wellbeing of staff, children and their families, and to ensure that Ferguson Park Pre-School operates in a professional and appropriate manner when using social media and/or information sharing platforms.

Staff must exercise extreme caution using digital technology facilities when accessing social media and/or information sharing platforms, whether in the workplace or relating to external events or functions involving Ferguson Park Pre-School.

It is a breach of confidentiality and privacy to make posts or comments about children, families, staff or management from Ferguson Park Pre-School on social media sites without consent or authorisation. It is also an offence under current legislation, to record or use a visual image of a child, including transmitting the image on the internet, without the written consent of the child's parent.

[Ferguson Park Pre-School] specifically requires that, unless you have the express permission, you:

- Do not video or photograph anyone, or post photos or personal details of other Ferguson Park Pre-School staff, children or families;
- Do not post photos or videos of Ferguson Park Pre-School staff, children or families on your personal Facebook page, or otherwise share photos or videos of staff, children or families through social media;
- Do not create a Ferguson Park Pre-School branded Facebook page, or other pages or content on social media that represents Ferguson Park Pre-School, it's staff, children or families without authorisation from the approved provider;
- Do not post anything that could embarrass or damage the reputation of Ferguson Park Pre-School, colleagues, children or families.

Staff must not:

- post or respond to material that is, or might be construed as offensive, obscene, fraudulent, defamatory, threatening, harassing, bullying, discriminatory, hateful, racist, sexist, infringes copyright, constitutes a contempt of court, breaches a Court suppression order, or is otherwise unlawful or inaccurate;
- make any comment or post any material that might otherwise cause damage to Ferguson Park Pre-School reputation or bring it into disrepute;
- imply that they are authorised to speak as a representative of Ferguson Park Pre-School, or give the impression that the views expressed are those of Ferguson Park Pre-School, unless authorised to do so
- use a Ferguson Park Pre-School email address or any Ferguson Park Pre-School logos or insignia that may give the impression of official support or endorsement of personal comments;
- use the identity or likeness of another employee, contractor or other member of Ferguson Park Pre-School;
- use or disclose any confidential information or personal information obtained in the capacity as an employee/contractor of Ferguson Park Pre-School; or
- access and/or post on personal social media during paid workhours.

Personal use of social media

Ferguson Park Pre-School recognises that staff may choose to use social media in their personal capacity. This policy is not intended to discourage nor unduly limit staff using social media for personal expression or other online activities in their personal life. Staff should be aware of and understand the potential risks and damage to Ferguson Park Pre-School that can occur through their use of social media, even if their activity takes place outside working hours or on devices not owned by Ferguson Park Pre-School.

If an individual can be identified as an employee of Ferguson Park Pre-School on social media, that employee must:

- only disclose and discuss publicly available information;
- ensure that all content published is accurate and not misleading and, complies with all relevant policies of Ferguson Park Pre-School
- expressly state on all postings (identifying them as an employee of Ferguson Park Pre-School) the stated views are their own and are not those of Ferguson Park Pre-School;
- be polite and respectful to all people they interact with;
- adhere to the Terms of Use of the relevant social media platform/website, as well as copyright,
- abide by privacy, defamation, contempt of Court, discrimination, harassment and other applicable laws;



- ensure that abusive, harassing, threatening or defaming postings which are in breach of Ferguson Park Pre-School policies may result in disciplinary action being taken, even if such comments are made using private social networks outside of working hours.
- notify the approved provider or person with management or control if they become aware of unacceptable use of social media as described above.

Consequences of unacceptable use of social media

- Ferguson Park Pre-School will review any alleged breach of this policy on an individual basis. If the alleged breach is of a serious nature, the person shall be given an opportunity to be heard in relation to the alleged breach.
- If the alleged breach is clearly established, the breach may be treated as grounds for dismissal. In all other cases, the person may be subject to disciplinary action in accordance with Ferguson Park Pre-School *Code of Conduct Policy*.
- Ferguson Park Pre-School may request that any information contained on any social media platform that is in breach of this policy be deleted.
- Ferguson Park Pre-School may restrict an employee's access to social media on [Ferguson Park Pre-School digital technology facilities or if they are found to have breached this policy or while Ferguson Park Pre-School investigates whether they have breached this policy.

ATTACHMENT 4. AUTHORISED USER AGREEMENT

Portable storage device (PSD) (including laptops)

I, _____,

- acknowledge that I have received a PSD belonging to Ferguson Park Pre-School
- will ensure that the PSD:
 - has no images of children, images to be stored in password protected USB
 - is used for work-related purposes only
 - is password-protected at all times
 - will not be loaned to unauthorised persons
 - will be returned to Ferguson Park Pre-School on cessation of employment
 - will not be used outside of Ferguson Park Pre-School unless an Authorised User Agreement is signed
- will notify the Nominated Supervisor or President as soon as is practicable if the PSD is damaged, faulty or lost
- have read the Ferguson Park Pre-School *Safe Use of Digital Technologies and Online Environment Policy* and agree to abide by the procedures outlined within.

Signature (authorised user)

Position

Date

Authorised by

Position

Date



ATTACHMENT 5. PARENT/GUARDIAN AUTHORISATION FOR UNDER-AGE ACCESS TO THE FERGUSON PARK PRE-SCHOOL DIGITAL TECHNOLOGY FACILITIES

Student's name:

Date of placement:

I, _____, am a parent/guardian of

I have read the Ferguson Park Pre-School *Safe Use of Digital Technologies and Online Environment Policy* and agree to the conditions of use of the service's digital technology facilities for the above-named student.

I also understand that Ferguson Park Pre-School provides no censorship of access to digital technology facilities.

Signature (student)

Date

Signature (parent/guardian)

Date



ATTACHMENT 6: ESSENTIAL PURPOSE AUTHORISATIONS FORM

Section 1: Personal Details

Staff Member Name:

Position:

Personal Device Type (e.g., Smartphone, Smart watch):

Date of use:

Section 2: Purpose

This form grants permission for the above-named staff member to use their personal device for the purposes of:

_____ at Ferguson Park Pre-School .

Section 3: Guidelines

1. Usage:

The National Model Code lists the following essential purposes for which the use or possession of a personal devices may be authorised where access does not impede the active supervision of children:

- communication in an emergency situation to ensure safety
 - involving a lost child, injury to child or staff member, or other serious incident
 - in the case of a lockdown or evacuation of the service premises
- personal health requirements
 - for example, heart or blood sugar level monitoring
- disability
 - for example, where a personal electronic device is an essential means of communication for an educator or other staff member
- family necessity
 - for example, an early childhood staff member with an ill family member
- technology failure
 - for example, when a temporary outage of service-issued electronic devices has occurred
- during a local emergency event to receive emergency notifications. This could include government warning systems such as a bushfire evacuation text notification.

2. Professional Conduct:

- Staff must maintain a professional demeanour while using personal devices.
- Authorised essential purpose authorisations form must be on file and accessible at all times.
- Devices should not be used for personal matters during work hours, unless authorised.

Section 4: Acknowledgement and Agreement

I, _____ (Staff Member Name), acknowledge that I have read, understood, and agree to comply with the guidelines outlined in this form. I understand the importance of protecting the privacy and security of the children in my care and the potential repercussions of failing to adhere to these guidelines.

Staff Member Signature:

| Date:

Approved Provide/Nominated Supervisor Name:

Approved Provide/Nominated Supervisor Signature:

| Date



ATTACHMENT 7: GUIDELINES FOR THE USE OF ARTIFICIAL INTELLIGENCE (AI) IN EARLY YEARS SERVICES

These guidelines are intended to support approved providers, service leaders, educators, and staff in the safe, ethical, and responsible use of Artificial Intelligence (AI) within early childhood education and care services, if they chose to use AI. AI technologies are often made by companies (often based overseas) whose primary focus is not children's rights and welfare. This should be considered when deciding whether or not to use them.

If choosing to use AI, the guidelines should be adapted to align with each service's philosophy, values, context, and obligations under the Child Safe Standards, the Privacy Act 1988 (Cth), and other relevant legislation and regulations.

Approved AI Systems

- Staff may only use AI systems that have been assessed and approved by the service and are included in the Approved AI Systems Register
- Approved systems will be regularly reviewed for capabilities, accuracy, security, and compliance with these guidelines.
- Staff wishing to suggest a new AI system for approval must submit it to the nominated supervisor or management for assessment.
- If staff become aware that a tool or platform in use has unapproved or hidden AI functionality, they must report it immediately.

Guidelines for AI Use

SUPERVISION AND PROFESSIONAL JUDGMENT

- AI should only be used as a supplementary tool to support administrative, educational, and operational tasks. It must not replace professional judgment or decision-making about children's learning, development, or wellbeing.
- All AI-generated outputs must be carefully reviewed and approved by a staff member before being used in practice or shared externally.

ACCURACY AND VERIFICATION

- Staff must remain vigilant for errors, inaccuracies, or bias in AI-generated content.
- Any inaccuracies identified in AI outputs must be corrected before the information is used.
- Human oversight is mandatory for all AI outputs to ensure alignment with the service's philosophy and ethical standards.

PRIVACY, DATA SECURITY, AND CONFIDENTIALITY

- Do not input confidential or personal information (names, birthdates, images or other identifying information) about children, families, or staff into AI systems
- Ensure that AI tools are configured to "do not use data to train machine learning models" where possible, to protect privacy.
- Only authorised personnel may access sensitive data, and it must be encrypted or securely stored when used in AI applications.
- Classify data based on sensitivity and apply appropriate levels of protection.
- Make sure any use of AI follows privacy laws.

CONSENT REQUIREMENTS

- Obtain managerial approval before using organisational or client data in AI applications.
- Where applicable, obtain informed consent from families if AI systems collect or process their data, clearly explaining:
 - What data will be collected.
 - How it will be used.
 - Their rights regarding the use of their data.

ETHICAL USE

- Use AI tools in ways that align with the service's values and ethical responsibilities.
- Avoid over-reliance on AI for educational or operational decisions.
- Ensure AI does not reinforce bias, discrimination, or inequity.



CONTENT CREATION

Educators use their deep knowledge and understanding of each child when planning and evaluating learning experiences. Over-reliance on AI to document children's experiences can reduce educators' meaningful connections with children's play and limit their ability to observe, reflect, and tailor learning to individual needs.

- AI may assist in generating ideas or drafting content but must not replace educators' professional expertise, relationships with children, or pedagogical decision-making.
- AI should only be used as a supportive tool; the final documentation and planning must be informed by educators' observations, insights, and pedagogical practices.
- Avoid directly copying and pasting AI-generated content; all outputs must be critically reviewed and adapted to reflect the unique context and voice of the service.
- Where AI has significantly contributed to content creation, this must be transparently acknowledged where appropriate.

Addressing the Limitations and Bias of AI

- AI systems are trained on large datasets that may not accurately reflect the diversity and inclusion values of the service or the community it serves. Educators must be aware of AI bias and critically review all outputs to avoid reinforcing discrimination or stereotypes.
- Risks of AI bias include:
 - Inaccurate or culturally unsafe content, particularly for underrepresented or marginalised communities such as Aboriginal and Torres Strait Islander peoples.
 - AI models reflecting only English-speaking, Western-centric values, which may not align with the diverse backgrounds of children, families, and educators.
 - "Hallucinations" (confident but incorrect or harmful AI-generated outputs) that require vigilant checking against approved learning frameworks (e.g., EYLF, MTOP, VEYLDF in Victoria).
- Educators must verify AI-generated content and ensure it aligns with the service's philosophy, curriculum, and ethical standards.

Operational Considerations

- Do not use AI systems for decisions involving child safety, wellbeing, or inclusion without managerial review.
- Review the content of apps, platforms, and tools used with children to ensure they are age-appropriate and safe.
- Remove access to AI systems immediately when a child leaves the service or a staff member exits their role.

Human-Led Self-Assessment and Continuous Improvement

Self-assessment is a vital process for services to reflect on their practices, engage with their community, and ensure continuous improvement.

- AI tools must not replace human-led self-assessment, as they are unlikely to provide insights specific to the service's unique circumstances and community perspectives.
- Services should ensure that all voices, including children, educators, families, and communities, are incorporated into reflective practices and quality improvement planning.

Record Keeping

- Maintain accurate records of:
 - The AI system used.
 - The priming instructions and inputs provided.
 - Any AI-generated outputs and the human review process.
 - Approvals from management or families (where applicable).

Review and Evaluation

- The service will regularly review and update these guidelines, approved AI systems, and associated procedures to ensure compliance with child safety and privacy standards.
- Feedback from staff and families will inform ongoing improvement.



ATTACHMENT 8: STORYPARK CONSENT FORM



FERGUSON PARK PRE-SCHOOL

4 GRAYSHARPS ROAD PO BOX 179, HURSTBRIDGE 3099

Phone: 9718 1571 Ferguson.park.kin@kindergarten.vic.gov.au

STORYPARK CONSENT FORM

Storypark is a safe and easy-to-use online communication tool. Only those invited to join the site will be able to do so. Ferguson Park Preschool uses Storypark to share children's learning, distribute group newsletters and message families.

Our program reflections contain photographs and text describing what the children are doing, the learning that is taking place and how the learning will be extended. Photos may be of individuals or groups of children working together. There may also be photos of family members participating in special events. Photographs/images on Storypark can be downloaded on personal devices by the authorised users. Therefore Ferguson Park Preschool uses a PDF version of photographs and images which cannot be downloaded.

Before using/posting any photos of your child on Storypark, we must first obtain your written consent. **Please read and sign the consent form below, indicating your preference, and return it to the kinder.** This form will be kept on file at Ferguson Park Preschool. You will also be asked to give consent when you first log on to Storypark.

Each child will have only **ONE** single account which is attached to a primary user. The primary user may extend accessibility to a second parent/carer.

PARENT/CARER CONSENT

Name of the child:

(Please tick the boxes)

I DO

I DO NOT

Give consent for my child to be included in individual and group photos that form part of a group learning story or group notice that can be viewed by other families in the kinder group.	☐	☐
Give consent for my child to be included in audios and videos (such as children singing a new song they've learned)	☐	☐
Give consent for my child to be included in photos attached to newsletters or notices viewed by the kinder community	☐	☐
Give consent for my child to have their portfolio linked to Ferguson Preschool's account and to be accessible by the educators at the service	☐	☐

I AGREE to respect the privacy of others and not share content, photos, videos or stories that feature children other than my own, without the written permission of those children's parents or guardians and act responsibly and not post inappropriate content in Storypark.

I understand that breaches to this agreement will be treated seriously and dealt with according to law.

Name of Primary User/Parent/Carer

Signature

Date





Ferguson Park Pre-School Educational Philosophy 2026



At Ferguson Park Pre-School, we provide an environment that is safe, inviting and inspiring. We are warm and caring, taking time to listen and be supportive to all children and their families. A service that is influenced by natural surroundings and embraces local and Aboriginal cultures.

The pre-school program recognises and caters for each child's individual needs. We encourage children to work together, as staff and children collaborate to explore and create. We provide challenges and opportunities that allow everyone to experience success.

Our educational program supports children to build fundamental social, emotional and communication skills, offering a range of hands-on experiences and targeted initiatives.

Our play-based program aims to foster high self-esteem, resilience confidence and a sense of belonging. There is a strong emphasis on children's sensitivity towards each other, on mutual respect for people in the wider community, and support for the social, cultural and religious diversity of families. At our pre-school, we believe that learning goes beyond the kinder room and is enhanced by the connections created with respect and acknowledgment of our wider community.

We offer learning experiences in a pleasing, natural, warm and nurturing learning environment which are child initiated as well and include intentional teaching objectives based on those interests. Our learning program evolves from a combination of these experiences, reflective practice and the children's voices. Ferguson Park Pre-School is committed to protecting our environment by implementing emerging sustainable practices with the children and kindergarten community.

We acknowledge the importance of parents, staff and other professionals, working together as partners, engaging in reflective discussions, researching, sharing, planning together to promote children's well-being, education, safe use of technology and development, preparing the children for a positive transition to school. Our families play an integral role in the planning and delivery of our service through our parent run volunteer committee and parent helpers.

Our center acknowledges and operates within the guidelines of the Victorian Child Safe Standards and the Early Years Learning Framework 2.0. This covers 5 educational outcomes:

1. **Children have a strong sense of identity**
2. **Children are connected with and contribute to their world.**
3. **Children have a strong sense of wellbeing.**
4. **Children are confident and involved learners.**
5. **Children are effective communicators.**

The policies and procedures for Ferguson Park Pre-School are guided by:

Education and Care services National Law 2010 and Education and Care Services Regulations 14th October 2011

Victorian Child Safe Standards, State of Victoria, Department of Health and Human Services, Revised in December 2019 and July 2022. National Model Code (SRE-NMC), September 2025



eSafety checklist for early learning services

Name of service: _____

Completed by (team or individual): _____

Checklist completed on (date): _____

Checklist shared with the service team on (date): _____

Aim

The aim of this checklist is to ensure that your early learning service has the processes, policies and practices to support a safe online environment. This includes making sure your service:

- understands the risks associated with being online for children, families, educators and the service more broadly
- provides experiences for children that help them learn and remember key strategies for being safe online
- supports staff through clear policies and practices
- works with families to share information about safe online practices at home and in the community
- has policies and procedures in place for the safe use of digital technologies and online environments, and takes reasonable steps to ensure they are followed
- follows the [National Model Code for Taking Images or Videos of Children while Providing Early Childhood Education and Care](#) (National Model Code)
- aligns with principle 8 of the [National Principles for Child Safe Organisations](#): Physical and online environments promote safety and wellbeing while minimising the opportunity for children and young people to be harmed
- identifies strengths and areas for improvement in current online safety measures, and documents them in [quality improvement plans](#).

How to use this checklist

eSafety's checklist for early learning services is organised into five sections:

- Policy
- Educational Program and Practice
- Infrastructure and Technology
- Educators
- Families

Each section has a list of questions to help you assess your service's policy, programs and practices for online safety considerations. Each question is referenced against the National Quality Framework (NQF), including the [Education and Care Services National Law \(National Law\)](#), the [Education and Care Services National Regulations \(National Regulations\)](#), the [National Quality Standard \(NQS\)](#) the [Early Years Learning Framework \(EYLF\)](#), and the [My Time, Our Place: The Framework for School Age Care \(MTOP\)](#). These can all form evidence for Assessment and Rating.

Go through each section and think about whether it reflects the way your service uses technology. Then tick the box that applies ('Yes', 'No' or 'Not yet') and write down examples or notes that help explain your decision. For example, if you tick 'Not yet', note who is responsible for completing it.

Please note: it is a requirement under National Regulations to have policies and procedures in place for the safe use of digital technologies and online environments at the service (regulation 168) and take reasonable steps to ensure those policies and procedures are followed (regulation 170). These policies and procedures must consider the following matters:

- The taking, use, storage and destruction of images and videos of children being educated and cared for by the service.
- Obtaining authorisation from parents to take, use and store images and videos of children being educated and cared for by the service.
- The use of any optical surveillance device at the service (for example, closed-circuit television).
- The use of any digital device issued by the service.
- The use of digital devices by children being educated and cared for by the service.

If you or your team need more information to answer parts of the checklist, refer to eSafety's Professional Learning Module: [Creating a Safe Learning Environment](#). This module explains the five checklist sections in more detail, features expert research, and links out to supporting documentation and examples. The checklist has been embedded in the module for ease of use.

Further information is available in the [NQF Online Safety Guide](#), which helps all staff understand and use digital technologies safely with children. This guide has a range of resources including the [NQF Online Safety Guide self-assessment and risk assessment tool](#).

These resources can be used along with this checklist to identify strengths and areas for improvement to include in [quality improvement plans](#).

Policy

Ensure your service has a written policy and procedures describing the safe use of digital technologies and online environments at your service.

Key questions	Check and explain		
Does your policy align with the National Model Code for Taking Images or Videos of Children while Providing Early Childhood Education and Care (National Model Code)? Does your policy adopt parts of the National Model Code, for example: - Only service-issued devices are to be used to take images or videos of children while providing education and care. - Personal electronic devices that can take images or videos, and personal storage and file transfer media, are not to be in the possession of any person while providing education and care and working directly with children, unless for authorised essential purposes such as emergencies, health and family needs. - Strict controls are to be in place for appropriately storing and retaining children's images and recordings.	Yes	No	Not yet
Does your policy clearly explain the rules for how children and educators should use technology and online platforms safety? This should cover things like: - age-appropriate access to technology - the taking of photos and videos - the use of service name/location on social media - personal and professional use of social media by employees. NQS: Element 7.1.2	Yes	No	Not yet
Does your policy detail procedures and processes around the taking, use, storage and destruction of images and videos of children being educated and cared for by the service? NQS: Element 7.1.2 National Regulations: regulation 168	Yes	No	Not yet
Does your privacy and confidentiality policy explain how the personal data (for example, names and photos) of children and families can be shared online (for example, by email, social media or cloud storage)? NQS: Element 7.1.2	Yes	No	Not yet

If your service uses an online parent communication tool, does its data storage and sharing procedure comply with relevant legislation, including the Privacy Act 1988 (Cth) or relevant state and territory legislation? To check, review the tool's privacy policy (this can usually be found in-app or on their website). Look for things like information on data storage (Australia or overseas), who has access, and how data is deleted when it is no longer needed. NQS: Element 7.1.2	Yes	No	Not yet
Does your policy require signed parent/ carer consent to take, use and store personal information, images and videos of children being educated and cared for by the service? NQS: Element 7.1.2 National Regulations: regulation 168	Yes	No	Not yet
Does your policy explain how children, educators and parents can raise concerns about digital technologies? NQS: Element 2.2.2	Yes	No	Not yet
Is there a clear process for recording breaches of policy? NQS: Element 2.2.2	Yes	No	Not yet
Does your policy have links to support agencies including eSafety, Kids Helpline, Headspace and Parentline? NQS: Element 2.2.2 EYLF: Practice – Holistic, integrated and interconnected approaches MTOP: Practice – Holistic, integrated and interconnected approaches	Yes	No	Not yet
Are there timelines for policy review? NQS: Element 7.2.1 EYLF: Principle – Critical reflection and ongoing professional learning MTOP: Principle – Critical reflection and ongoing professional learning	Yes	No	Not yet

Educational program and practice

Ensure your service has online safety principles embedded in your program and practice.

Key questions	Check and explain		
Does your service provide children with the opportunity to engage in digital play through communicating, creating and consuming digital content in safe and developmentally appropriate ways? NQS: Element 1.1.1 EYLF: Learning outcome – Children are confident and involved learners MTOP: Learning outcome – Children and young people are confident and involved learners	Yes	No	Not yet
Do your educators regularly discuss concepts of ‘being online’ or ‘the internet’ with children so that they continue to develop their understanding? NQS: Element 1.2.1 EYLF: Learning outcome – Children have a strong sense of identity MTOP: Learning outcome – Children and young people have a strong sense of identity	Yes	No	Not yet
Do your educators teach and regularly remind children about online safety (for example, asking permission before they take a photo)? NQS: Element 1.2.2 EYLF: Learning outcome – Children have a strong sense of wellbeing MTOP: Learning outcome – Children and young people have a strong sense of wellbeing	Yes	No	Not yet
Do children know what to do if they encounter inappropriate materials online? NQS: Element 5.2.2 EYLF: Learning outcome – Children are effective communicators MTOP: Learning outcome – Children and young people are effective communicators	Yes	No	Not yet
Is online behaviour included in discussions and activities promoting respectful relationships? NQS: Element 5.2.2 EYLF: Learning outcome – Children are confident and involved learners MTOP: Learning outcome – Children and young people are confident and involved learners	Yes	No	Not yet

Infrastructure and technology

Ensure your service has online safety principles embedded in your program and practice.

Key questions	Check and explain		
Do you have a record of all the technologies you have in your service, and which of these are connected to the internet? NQS: Element 7.1.2	Yes	No	Not yet
Do the devices at your service have filters or settings that block harmful or adult content, and do you have monitoring in place to ensure that devices are being used safely? NQS: Element 7.1.2	Yes	No	Not yet
Are your device settings at a level of privacy that reflects data protection laws? Data protection laws (such as the Privacy Act 1988) mean that you must only collect information you need (don't gather extra personal data 'just in case'), keep it secure (for example, passwords, encryption), share it only with consent (unless legally required), and delete or de-identify it when it's no longer needed. NQS: Element 7.1.2	Yes	No	Not yet

Educators

Ensure your educators model safe online practices for young children and know your service's online safety policies.

Key questions	Check and explain		
Do your educators provide adequate supervision when young children are using digital technology? NQS: Element 2.2.1 EYLF: Practice – Responsiveness to children MTOP: Practice – Collaboration with children and young people National Law: section 165	Yes	No	Not yet
Have your educators engaged in professional learning about online safety (such as eSafety's professional learning modules and the NQF Online Safety Guide), enabling them to identify and mitigate the risks associated with being online? NQS: Element 7.2.3; EYLF: Practice – Continuity of learning and transitions MTOP: Practice – Continuity and transitions	Yes	No	Not yet
Do you provide educators with regular opportunities to engage in ongoing, informal professional learning (for example, updates at staff meetings, sharing short resources) so they have up-to-date information about the risks and changing practices in online safety? NQS: Element 7.2.3; EYLF: Principle – Critical reflection and ongoing professional learning MTOP: Principle – Critical reflection and ongoing professional learning	Yes	No	Not yet
Are your educators aware of (and compliant with) your guidelines around privacy and their use of social media for both professional and personal purposes? NQS: Element 7.2.3; EYLF: Principle – Critical reflection and ongoing professional learning MTOP: Principle – Critical reflection and ongoing professional learning	Yes	No	Not yet
Do you regularly involve educators in the development and review of your online safety policies? NQS: Element 7.2.1; EYLF: Principle – Critical reflection and ongoing professional learning MTOP: Principle – Critical reflection and ongoing professional learning	Yes	No	Not yet

Families

Ensure your service is providing regular, quality information to your families about being safe online.

Key questions	Check and explain		
Do you have a parent-engagement strategy to communicate appropriate online safety information? NQS: Element 6.1.1; EYLF: Principle – Partnerships with families MTOP: Principle – Partnerships	Yes	No	Not yet
Are there processes in place to ensure children and parents/carers who speak languages other than English understand your online safety policy? NQS: Element 6.1.3 EYLF: Practice – Cultural responsiveness MTOP: Practice – Cultural responsiveness	Yes	No	Not yet
Does your policy explain how families can raise online safety issues in appropriate ways (for example, through agreed communication channels such as email or meetings)? NQS: Element 6.1.3 EYLF: Principle – Partnerships MTOP: Principle – Partnerships	Yes	No	Not yet
Have you involved parents/carers in the development and review of your online safety policies (for example, through surveys, inviting feedback or holding short information sessions)? NQS: Element 6.1.1 EYLF: Principle – Partnerships MTOP: Principle – Partnerships	Yes	No	Not yet
Do you provide your families with information on where to go for help with online safety issues, including eSafety? NQS: Element 6.1.3 EYLF: Principle – Partnerships MTOP: Principle – Partnerships	Yes	No	Not yet

When this checklist has been completed, ensure it is shared with educators and families to show them what your service is doing to improve children's online safety. You might do this through a staff meeting, newsletter, family information session, or by putting a summary on your noticeboard. You can also share key points with community partners (such as local schools) to help keep messaging about online safety consistent as children move from early learning into primary school.

Ensure this checklist is reviewed and updated regularly to reflect advances in technology, new online safety resources and data protection laws.

Date for review and update: _____

CHILD SAFETY

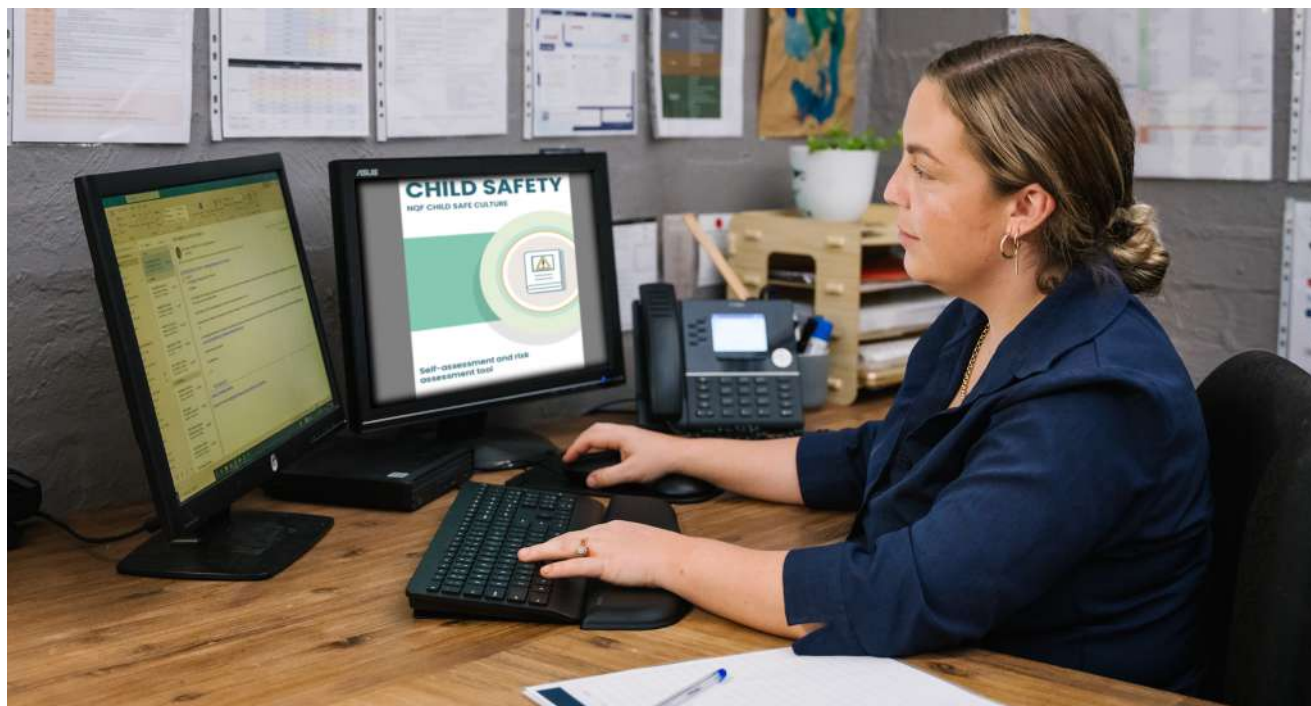
NQF CHILD SAFE CULTURE



**Self-assessment and risk
assessment tool**

NQF Child Safe Culture

Self-assessment and risk assessment tool



This voluntary self-assessment and risk assessment tool will support approved providers, service leaders, educators and all staff in children's education and care services to:

- reflect on the service's child safe culture and practices and
- identify strengths and areas for improvement to include in quality improvement plans
- identify risks and priority areas for improvement and risk management.

It is recommended approved providers and service leaders use this tool with educators and other staff, alongside the guidance provided in the [NQF Child Safe Culture Guide](#) (the Guide), to review the service's child safe culture and identify areas where they are doing well, potential risks and areas for improvement. Each theme explored in this tool is supported by the content in the relevant chapter of the Guide.

Users should consider how their practices are aligned to the National Quality Framework (NQF), [National Principles for Child Safe Organisations](#) (National Principles) and where relevant, mandatory Child Safe Standards (CSS) in the state/territory where they are located. The resources section of each chapter of the Guide includes relevant connections to the NQF, National Principles and CSS.

Self-assessment and risk assessment tool

This tool can be used by approved providers and service leaders:

- In teams, to discuss and prioritise the safeguarding systems, beliefs and practices at your service.
- To assess how your service is meeting its child safe obligations and think about the way you work with children, young people and families to be vigilant in maintaining a child safe culture.
- To inform leadership decisions and plan professional development and ongoing management of staff.
- To reflect on how to:
 - improve practice
 - support critical reflection
 - identify and mitigate risks
 - embed child safe practices across your service.

When using the tool, include those who understand the day-to-day activities, practices, policies and procedures as well as engaging with service leaders, staff, educators and volunteers at your service. Also, consulting with children, families and the community to gather a diverse range of perspectives and experiences can strengthen your reflective conversations and support a strong child safe culture at your service.

Self-assessment and risk assessments should be undertaken on a regular basis, at least annually, and be reviewed following any incidents. If the service leader is completing the tool with the service team, it is recommended that the approved provider also review the completed tool.

Use the [NQF Child Safe Culture Guide](#) to help you complete the tool and consider future actions.

Note there is also an [NQF Online Safety - Self-assessment and risk assessment tool](#) specifically to assist with online safety in children's education and care services.

Self-assessment and risk assessment tool

How to use this tool:

1. Select the theme you want to focus on e.g. *1. Building a Child Safe Culture*
2. Read the Statement and Prompts in the tool. The Prompts are examples of practices and strategies you could be using, to help you reflect on the Statement.

1. Building a Child Safe Culture	
Statement	Prompts
Our service implements practices to create and maintain a child safe culture	• We have and implement policies and procedures that... • Other: [please add your own Prompts]

3. Record whether the Prompts are true for your service 'always', 'most of the time', 'sometimes', 'rarely' or 'never'.
4. Record 'other' if you don't know or are unsure.
5. There is space for adding additional Prompts under 'other' in the list. This is where you can add your own items relevant to your service or draw other Prompts from the relevant chapter of the [NQF Child Safe Culture Guide](#).

Our service does this: (select one)	Always	Mostly	Sometimes	Rarely	Never	Other (Unsure)
	☐	☐	☐	☐	☐	☐

6. Complete steps 1 to 4 for each Statement and its set of Prompts within the theme.
7. Review your responses. Consider each response and identify areas of strength, where child safety is well managed across your service.
 - a. You can copy and paste the Prompts that your service does well – adding additional rows as needed.
 - b. You may also want to include examples or note evidence of this practice in your service.

Strengths	[example/evidence of Prompt in your service]

8. Review the areas where you've selected 'sometimes', 'rarely', 'never' or 'other' and identify areas for improvement and a level of priority.

Self-assessment and risk assessment tool

Areas for improvement		Priority		
		Low	Med	High
1.		☐	☐	☐
2.		☐	☐	☐
3.			☐	☐

- Where relevant, transfer the strengths, examples and areas for improvement to your standard Self-assessment tool and/or Quality Improvement Plan (QIP) against the relevant quality area or standards in your standard NQS self-assessment tool and/or QIP.
- If you have identified areas for improvement that indicate there are existing or potential risks to the safety, health or wellbeing of children at your service, complete the risk assessment and make a plan to address identified risk(s).

How to use the Risk Assessment tool:

- Undertake a risk assessment of the areas for improvement for all existing or potential risks to the safety, health or wellbeing of children including **hazards, concerns or risk of harm** identified during your self-assessment. (See the [ACECQA Risk Assessment and Management tool](#) for definitions of key terms including risk and hazard.)
- Consider the **level of risk** areas for improvement may present for children, families, staff or as barriers to developing a child safe culture across your service. The Risk Matrix below can assist you in identifying the level of risk.
- For service leaders and approved providers: Plan **control measures** for how these risks can be managed, reduced or eliminated, **noting who will be responsible** for actioning these and **when** they will be actioned.

Risk assessment					
Activity	Hazard/risk of harm identified	Risk assessment (use matrix)	Control measures	Who?	When?

- After the risk assessment is complete, service leaders should prepare and review the service's policies and procedures and address risks identified in the child safe culture risk assessment.
- Schedule regular reviews and update your risk assessment at least once every 12 months and as soon as practicable after becoming aware of any circumstance that may affect the safety, health or wellbeing of children, as hazards, concerns or risk of harm may change.

Self-assessment and risk assessment tool

Risk matrix:

A risk matrix is a useful tool to use during the risk assessment process. It helps in identifying the level of risk by looking at the **likelihood** that an event may occur, and the severity of the **consequences** should it occur.

The [Guide to the NQF](#) defines likelihood and consequences in a risk matrix in [[Section 5: Regulatory Authority powers](#)].

Risk Matrix						
		Likelihood				
Consequences		Rare	Unlikely	Possible	Likely	Almost
	Major	Moderate	High	High	Critical	Critical
	Significant	Moderate	Moderate	High	High	Critical
	Moderate	Low	Moderate	Moderate	High	High
	Minor	Very low	Low	Moderate	Moderate	Moderate
	Insignificant	Very low	Very low	Low	Moderate	Moderate

If you need more information on conducting a risk assessment, refer to ACECQA's [Risk Assessment and Management tool](#).

A [checklist for education and care services](#) is available on the eSafety website, and further [Child Safety Risk Management Resources](#) are available on the National Office for Child Safety website.

Self-assessment and risk assessment tool

Contents of the tool:

1. Building a child safe culture	8
2. Leadership, policies and continuous improvement	12
3. Child’s voice and cultural safety	15
4. Protective behaviours and child safe pedagogy	20
5. Recruitment	25
6. Induction, probation and ongoing staff management	29
7. Professional development.....	32
8. Complaints and disclosures	35
9. Families and the community	38

Self-assessment and risk assessment tool

Child Safe Culture Self-assessment and Risk Assessment Tool

Name of Service:

Date completed:

Participants:

Review date set:

1. Building a child safe culture

Statement	Prompts
a) Our service implements practices to create and maintain a child safe environment and promotes a culture of child safety and wellbeing.	• Everyone involved in the service promotes and demonstrates their commitment to a culture of child safety, which reflects the NQF, and embeds the National Principles for Child Safe Organisations and jurisdiction-specific Child Safe Standards. • We establish an effective and consistent approach to child safety with risk management practices to prevent, identify, respond to and report allegations or concerns about child maltreatment, abuse or neglect. • We regularly review and critically reflect on our service's philosophy, policies and procedures with all staff members to ensure all staff, educators, volunteers, service leaders and the approved provider maintain their understanding of ethically and culturally safe practices, their roles and responsibilities, and update as necessary. • We consider the setting, number, ages and development stages of children being educated and cared for, including at each education and care service and Family Day Care (FDC) residence or approved FDC venue of the service. • We consider children's safety in all decisions made at the service. • We discuss shared values and behaviours that promote all staff's understanding of child safety and the maintenance of a child safe culture across the service (offline and online). • We discuss the responsibilities we hold to raise any concerns and the processes for doing so. • We regularly undertake self-assessments of the service's culture and how the service is creating and promoting a child safe environment and safeguarding all children, and identify areas for improvement. • Other:

Self-assessment and risk assessment tool

Our service does this: (select one)	Always	Mostly	Sometimes	Rarely	Never	Other (Unsure)
Strengths						
Areas for improvement						Priority
						Low Med High
1.						
2.						
3.						
Statement	Prompts					
b) Our child safeguarding (preventative) practices consider children's views and voices, culturally safe practices, and family and community contexts.	- We seek, listen to and respect children's voices, views and opinions before making a decision that impacts them. - We talk to children about their rights in an age and developmentally- appropriate way, including their rights to speak, talk about things that concern them and/or make a complaint when they feel unsure, uncomfortable or unsafe. - We provide culturally safe and responsive services for children and families, particularly for Aboriginal and Torres Strait Islander children and families, culturally and linguistically diverse children and children with additional needs. - To help us recognise when a child may be at increased risk, we know and understand our service's families, community and context and implement protective behaviours, including having appropriate and culturally safe discussions with families. - Other:					

Self-assessment and risk assessment tool

Our service does this: (select one)	Always	Mostly	Sometimes	Rarely	Never	Other (Unsure)
Strengths						
Areas for improvement						Priority
						Low Med High
1.						
2.						
3.						
Statement	Prompts					
c) Our service leaders, educators and staff members are confident in how to respond to concerns of alleged or suspected child abuse or harm.	- We recognise how a child's presentation, behaviour, reactions or things they say may change if they have experienced maltreatment, abuse or neglect (in both offline and online settings). - We ensure everyone connected with the service is aware of how to raise an issue or concern or make a complaint within our service/organisation. - We ensure all staff and volunteers understand their mandatory reporting obligations and how to make a report to a child protection agency and their Regulatory Authority. - We take seriously and respond to any direct, indirect or suspected disclosure of child abuse or harm, including through using trauma-informed practice. - Other:					

Self-assessment and risk assessment tool

Our service does this: (select one)	Always	Mostly	Sometimes	Rarely	Never	Other (Unsure)
Strengths						
Areas for improvement					Priority	
					Low	Med
1.						
2.						
3.						

Risk Assessment	Consider the areas for improvement. Have you identified any hazards or potential risk of harm? If yes, complete the following risk assessment to plan your response.				
	Yes	No			
Activity	Hazard/risk of harm identified	Risk assessment (use matrix)	Control measures	Who?	When?

Self-assessment and risk assessment tool

2. Leadership, policies and continuous improvement

Statement	Prompts					
a) Our leadership team models a child safe culture.	• The approved provider and service leaders work together to model positive child safeguarding attitudes and behaviours, and promote child safe pedagogical practices. • The approved provider and service leaders clearly and effectively prioritise and communicate child safety matters, advocate for children's right to feel safe and demonstrate their commitment to keeping children safe. • Our leadership team lead by example and find ways to improve child safety, including identifying and addressing risks before they become problems. • Each member of staff, including volunteers and students feels supported and encouraged to raise concerns and knows the process for raising concerns about practices that put children at risk of harm. • The approved provider and service leaders take child safety issues seriously, respond quickly, and ensure all staff and volunteers have the resources they need to maintain child safe practices at all times. • We ensure other organisation/s or personnel working with children in our care, such as students, volunteers or visitors, are considered in our policies and procedures and are aware of their responsibilities. • Other:					
Our service does this: (select one)	Always	Mostly	Sometimes	Rarely	Never	Other (Unsure)
Strengths						

Self-assessment and risk assessment tool

Areas for improvement		Priority		
		Low	Med	High
1.				
2.				
3.				

Statement	Prompts
b) Our service policies and procedures prioritise providing a child safe environment and promoting a culture of child safety, including through our Code of Conduct and Statement of Philosophy.	• We make sure all policies and procedures prioritise providing a child safe environment and promoting a culture of child safety, and include the National Principles and relevant state/territory Child Safe Standards. • Our policies and procedures include information about responsibilities and processes regarding concerns or allegations of child maltreatment, abuse or neglect for approved providers, service leaders, all staff, volunteers and students, including reporting obligations. • Our policies and procedures include preventative actions to support child safeguarding and responding to child safety concerns. • We regularly review child safety policies and practices ensuring everyone knows and follows them and seek feedback from everyone, including children, families, and the community. • Our Code of Conduct is easy to access and understand, is included in induction and training and is reflected on in ongoing discussions about child safety. • Our Statement of Philosophy reflects the National Principles/ Child Safe Standards, UN Convention on the Rights of the Child and our commitment to child safety. • Other:

Self-assessment and risk assessment tool

Our service does this: (select one)	Always	Mostly	Sometimes	Rarely	Never	Other (Unsure)
Strengths						
Areas for improvement					Priority	
					Low	Med
1.						
2.						
3.						

Risk Assessment	Consider the areas for improvement. Have you identified any hazards or potential risk of harm? If yes, complete the following risk assessment to plan your response.				
	Yes	No			
Activity	Hazard/risk of harm identified	Risk assessment (use matrix)	Control measures	Who?	When?

Self-assessment and risk assessment tool

3. Child's voice and cultural safety

Statement	Prompts
a) The approved provider, service leaders and educators, staff work to develop children's voices and their ability to communicate and be heard, listened to and believed.	- We promote a child-centred, rights-based, respectful, child safe culture where children are aware of their right to say 'no' and can raise concerns and those concerns are listened to and taken seriously, acknowledged, respected and responded to. - We listen to, respect and respond to children's voices, including their non-verbal cues. - We have resources and programs to educate and inform children of their rights, including their rights to safety and we share information about how the service keeps them safe in a developmentally appropriate way. - Our educators support children's body safety awareness through education and understanding of their rights to say no to any activities that make them feel uncomfortable, unsure or unsafe. - Our service provides resources or pathways for children and families to access support services when needed. - Other:

Our service does this: (select one)	Always	Mostly	Sometimes	Rarely	Never	Other (Unsure)
Strengths						
Areas for improvement					Priority	
					Low	Med
1.						
2.						
3.						

Self-assessment and risk assessment tool

Statement	Prompts					
b) Our service strives to ensure children are active citizens and feel empowered and confident to participate in decisions that impact their learning and experiences.	• We provide children with opportunities to feel valued and make choices during their time while at the service. • We support children to feel they belong and feel safe while interacting with staff and other children at the service. • We support children to know they can raise concerns and interact with trusted adults if they feel unhappy, unsure or unsafe. • We embed a culture where children can talk about their feelings, emotions and safety and the safety of other children. • We have a culture where children participate, are listened to and their views have an impact on the way the service operates. • We seek, listen to, support, and act upon the voices, views and opinions of Aboriginal and Torres Strait Islander peoples. • We foster a culturally safe environment that empowers Aboriginal and Torres Strait Islander children to speak, with trust that their voices will be heard and respected. • We ensure policies and procedures reflect and protect the rights of children from culturally and linguistically diverse (CALD) backgrounds, children with additional needs, and children who identify as LGBTIQ+ so they can freely talk about concerns around their safety and the safety of other children. • We explain the context of a situation to children, ask them questions in different ways, and give them different opportunities to contribute • We provide time for children to express themselves, to clarify what they mean and to provide feedback. • We teach children about acceptable behaviour in both physical and online environments. • Other:					
Our service does this: (select one)	Always	Mostly	Sometimes	Rarely	Never	Other (Unsure)
Strengths						

Self-assessment and risk assessment tool

Areas for improvement	Priority			
	Low	Med	High	
1.				
2.				
3.				

Statement	Prompts
c) Our educators and staff members demonstrate equity and respect for diversity.	- We have child-friendly materials in a number of accessible languages and formats available to children. - We promote inclusive approaches to the raising of concerns and making of complaints to ensure all children, regardless of their abilities, can be heard. - We champion attitudes and behaviours that respect the rights of all children, and are inclusive, evidence-informed and responsive to diverse needs. - We actively discourage discrimination against children, families and educators on the basis of culture, gender, age, sexuality, disability or religion. - We support all children, including those with diverse needs, backgrounds and family formations, to voice concerns around their safety and the safety of other children. - We work with all staff members to reflect on and address any intentional or unintentional bias, discrimination and exclusion at the service. - Other:

Our service does this: (select one)	Always	Mostly	Sometimes	Rarely	Never	Other (Unsure)
Strengths						

Self-assessment and risk assessment tool

Areas for improvement	Priority		
	Low	Med	High
1.			
2.			
3.			

Statement	Prompts
d) Our service values and works to embed Aboriginal and Torres Strait Islander cultures and perspectives.	- We regularly reflect on how the service embeds Aboriginal and Torres Strait Islander perspectives and identify ways to create, and improve on, a culturally safe environment where Aboriginal and Torres Strait Islander children and families feel respected, empowered to speak and trust they will be heard. - We seek guidance from Aboriginal and Torres Strait Islander staff, Elders and community members to ensure their perspectives are reflected in our service's Statement of Philosophy, policies and procedures and Quality Improvement Plan (QIP). - We support, listen to and act on the views and opinions of Aboriginal and Torres Strait Islander children to ensure all children feel respected and proud of their identities and cultures. - We include local Aboriginal and Torres Strait Islander knowledge, perspectives and language learning for all children, including through visual resources. - Other:

Our service does this: (select one)	Always	Mostly	Sometimes	Rarely	Never	Other (Unsure)

Strengths

Self-assessment and risk assessment tool

Areas for improvement		Priority		
		Low	Med	High
1.				
2.				
3.				

Risk Assessment		Consider the areas for improvement. Have you identified any hazards or potential risk of harm? If yes, complete the following risk assessment to plan your response.			
		Yes	No		
Activity	Hazard/risk of harm identified	Risk assessment (use matrix)	Control measures	Who?	When?

Self-assessment and risk assessment tool

4. Protective behaviours and child safe pedagogy							
Statement	Prompts						
a) Educators, staff members and volunteers know how to identify and respond to harmful sexual behaviour.	- We make sure educators, staff members volunteers and students are aware of the range of indicators of child maltreatment, abuse and neglect. - We make sure educators, staff members volunteers and students are aware of reporting obligations and have confidence to respond and act on complaints or disclosures from children and others. - We ensure educators, staff members, volunteers and students understand the continuum of children's sexual behaviour and the difference between developmentally expected sexual behaviour and problematic, concerning and harmful behaviour by children or between children. - We respond appropriately when concerns are raised about sexual behaviours displayed (in both offline and online settings). - We discuss and share information with families about child development and child safety resources as part of ongoing education and support for children and families. - Other:						
Our service does this: (select one)	Always	Mostly	Sometimes	Rarely	Never	Other (Unsure)	
Strengths							
Areas for improvement					Priority		
					Low	Med	High
1.							
2.							
3.							

Self-assessment and risk assessment tool

Statement	Prompts					
b) Our service understands and ensures effective supervision contributes to child safety.	• We consider child-specific factors to ensure active supervision is effective, including: • each child's circumstances • the abilities and individual needs of each child • the dynamics of each group of children. • When supervising children, we work together to consider and understand risk in physical and online environments and foster a shared understanding through effective communication. • We understand that children of different ages and abilities, undertaking different activities (including excursions, regular outings and during transportation), need different levels of supervision, and we adapt our supervision strategies, levels and risk assessments appropriately. • We consider the arrangement of rooms, learning spaces and equipment indoors and outdoors, to ensure line of sight and effective supervision for, and of, all staff and children. • We ensure the suitability of staffing arrangements required to adequately and effectively supervise and monitor children across the service, including during transitions. • In FDC, we consider that children of different ages might need different levels or types of supervision, and may also be in different parts of the approved FDC premises. • In OSHC, we effectively supervise children and show respect for the age range of children going to and from toilets and bathroom spaces. • In OSHC, we ensure appropriate supervision during the transition between school or another venue to the OSHC service. • Other:					
Our service does this: (select one)	Always	Mostly	Sometimes	Rarely	Never	Other (Unsure)
Strengths						

Self-assessment and risk assessment tool

Areas for improvement	Priority		
	Low	Med	High
1.			
2.			
3.			

Statement	Prompts
c) Educators and staff members foster responsive, inclusive and appropriate behaviour guidance for children at our service.	- The approved provider and their service leaders work to build an effective workforce which fosters nurturing and responsive relationships with children and families. - The approved provider and service leaders support educators and staff members to undertake training to be proactive in implementing positive behaviour guidance strategies. - The approved provider, all staff, volunteers, and students at our service feel confident to intervene when a colleague is struggling or acting inappropriately with children and to report concerning behaviour, interactions or inappropriate conduct. - We develop and critically reflect on the service's philosophy and related policies and procedures which include appropriate strategies to guide and support each child's behaviour in positive and productive ways. - We plan for the inclusion of every child, including those who may have diagnosed behavioural or learning challenges. - Other:

Our service does this: (select one)	Always	Mostly	Sometimes	Rarely	Never	Other (Unsure)
Strengths						

Self-assessment and risk assessment tool

Areas for improvement	Priority		
	Low	Med	High
1.			
2.			
3.			

Statement	Prompts
d) Approved providers and their service leaders support educators' child safety pedagogy.	- We provide regular training on child safety policies and evidence-based practices, including cultural safety. - We encourage educators to discuss and critically reflect on their pedagogy and how it supports child safe practice. - We provide a supportive environment for educators, staff members, volunteers and students who disclose harm or risk of harm to children by colleagues, including through debriefs and providing referrals for additional support. - We ensure educators, volunteers and other staff members at all levels understand how to identify and respond effectively when concerns or issues of child maltreatment, abuse or neglect arise, including mandatory reporting obligations. - Other:

Our service does this: (select one)	Always	Mostly	Sometimes	Rarely	Never	Other (Unsure)

Strengths

Self-assessment and risk assessment tool

Areas for improvement		Priority		
		Low	Med	High
1.				
2.				
3.				

Risk Assessment		Consider the areas for improvement. Have you identified any hazards or potential risk of harm? If yes, complete the following risk assessment to plan your response.			
		Yes	No		
Activity	Hazard/risk of harm identified	Risk assessment (use matrix)	Control measures	Who?	When?

Self-assessment and risk assessment tool

5. Recruitment						
Statement	Prompts					
a) When creating or reviewing recruitment policies and procedures we ensure child safety and children's voices are considered and reflected.	- We ensure recruitment policies and procedures have a child safe focus. - We use interview questions that explore the applicant's practices and professional beliefs and how they align with the service's child safe culture. - We ensure child safety is at the core of the recruitment process and that each position description includes child safety requirements and elements. - We recognise the risks to children's safety, and to the service more broadly, if applicants who do not share our child safety values and practices are recruited. - The approved provider and service leaders understand their role in leading recruitment practices that are focussed on child safety. - Other:					
Our service does this: (select one)	Always	Mostly	Sometimes	Rarely	Never	Other (Unsure)
Strengths						
Areas for improvement					Priority	
					Low	Med
1.						
2.						
3.						

Self-assessment and risk assessment tool

Statement	Prompts					
b) When creating position descriptions, recruitment advertisements and reviewing applications, we are transparent about our services commitment to child safety, inclusivity and culturally safe practices.	• We ensure effective child safe practices are at the centre of staff recruitment. • As part of our child safe culture, our service is clear and explicit about the role and responsibilities of each educator, volunteer, student and other staff members, including mandatory reporting. • Our service has clear expectations, included in position descriptions and advertisements, which explain that individuals must demonstrate the following experiences, behaviours and practices: • a commitment to child safety • respect and value children • understanding or a willingness to learn about and support children's developmental needs • culturally safe practices. • Our service reviews applications and makes decisions about interviewing applicants who prioritise children's safety and whose values align with the child safe practices of the service. • Other:					
Our service does this: (select one)	Always	Mostly	Sometimes	Rarely	Never	Other (Unsure)
Strengths						

Self-assessment and risk assessment tool

Areas for improvement	Priority		
	Low	Med	High
1.			
2.			
3.			

Statement	Prompts
c) When creating, then undertaking interviews and conducting post interview checks, we consider our services commitment to child safety, inclusivity and culturally safe practices.	- We have well-understood processes in place to look for potential warning signs and inconsistencies in applications, interviews and appropriate checks are undertaken prior to any offer of employment being made. - We include specific child safety questions in interview processes to ensure applicants are suitable. - Our service takes time to reflect on answers provided by applicants in interviews and assess their suitability to join our service, rather than rushing to fill positions. - We undertake the required background checks for all staff (including volunteers and students) at the service prior to commencement, including: - working with children or vulnerable persons checks, - fit and proper checks for relevant persons in FDC residences, and - a prohibited persons register search. - We ensure recruitment agencies understand our child safe policies and expectations for recruitment, and that they undertake the required checks, including verbal referee checks, for all applicants. - Other:

Our service does this: (select one)	Always	Mostly	Sometimes	Rarely	Never	Other (Unsure)
Strengths						

Self-assessment and risk assessment tool

Areas for improvement		Priority		
		Low	Med	High
1.				
2.				
3.				

Risk Assessment		Consider the areas for improvement. Have you identified any hazards or potential risk of harm? If yes, complete the following risk assessment to plan your response.			
		Yes	No		
Activity	Hazard/risk of harm identified	Risk assessment (use matrix)	Control measures	Who?	When?

Self-assessment and risk assessment tool

6. Induction, probation and staff management

Statement	Prompts					
a) Child safety and culturally safe practices are central to our service's induction and probation processes for new educators, and all staff members, volunteers and students.	• Our service ensures child safety is at the core of induction for persons with management and control, service leadership, educators and other staff members, volunteers and students. • We provide access and opportunities for all staff members to discuss and clarify our service's guiding documents. • We support new staff members to understand how they meet their child safety related record keeping, information sharing and reporting responsibilities, including how they can report concerns within the service and how these will be managed. • In our induction processes, we ensure educators understand and know how to implement child safe practices that are reflected in the Approved Learning Frameworks (ALFs), including the EYLF and MTOP (and VEYLDF for services in Victoria). • Discussion of the service's child safe culture and practices is included as a standing agenda item for staff meetings. • We hold regular sessions (including refresher training) for educators and staff members to confirm their understanding and application of child safety, including examples from within our service. • We provide opportunities for new team members to safely explore their views about child safe practices with a designated staff member (for example a buddy, room leader, mentor or area manager with appropriate knowledge and expertise), who will listen to and respond to questions. • We ensure effective child safe practices are at the centre of induction and management of staff. • Other:					
Our service does this: (select one)	Always	Mostly	Sometimes	Rarely	Never	Other (Unsure)
Strengths						

Self-assessment and risk assessment tool

Areas for improvement		Priority		
		Low	Med	High
1.				
2.				
3.				

Statement	Prompts
b) Ongoing supervision and support for educators, other staff members and volunteers aligns with our service's child safe culture, policies and procedures.	- The approved provider and service leaders ensure our child safety culture and practices are discussed as a core element in staff supervision. - We provide ongoing professional development for all educators and staff members to help them grow and maintain the service's child safe culture, policies and procedures, covering: - The National Principles for Child Safe Organisations training and, where it exists, training on mandatory state/territory Child Safe Standards - child maltreatment, abuse and neglect prevention, recognition, reporting, response and trauma-informed practices - appropriate behaviour guidance. - The approved provider and service leaders continuously support, mentor and supervise all educators, staff, volunteers and students to meet their child safety responsibilities. - All staff act immediately to address warning signs and early indicators of inappropriate behaviours between children, and inappropriate staff behaviour towards children. - We ensure those supervising other staff are supported and have the appropriate tools and training to discuss and record Code of Conduct and policy breaches, and poor interactions with children. - We ensure those supervising other staff know the actions to take for concerning behaviour or inappropriate conduct of staff or volunteers. - Our Code of Conduct and Service Philosophy reflect the service's commitment to providing a child safe culture and are implemented by all staff. - We maintain an active review process for all staff (including volunteers and students) at the service to ensure they remain suitable for employment, including working with children or vulnerable persons checks, fit and proper checks for relevant persons in FDC residences, and a prohibited persons register search. - Other:

Self-assessment and risk assessment tool

Our service does this: (select one)	Always	Mostly	Sometimes	Rarely	Never	Other (Unsure)
Strengths						
Areas for improvement					Priority	
					Low	Med
1.						
2.						
3.						

Risk Assessment		Consider the areas for improvement. Have you identified any hazards or potential risk of harm? If yes, complete the following risk assessment to plan your response.			
		Yes	No		
Activity	Hazard/risk of harm identified	Risk assessment (use matrix)	Control measures	Who?	When?

Self-assessment and risk assessment tool

7. Professional development

Statement	Prompts					
a) Our service supports educators, other staff members, and volunteers' ongoing child safety education and professional development.	• All staff keep up to date with the latest child safety information and any changes under the NQF and state or territory child safety requirements. • Where required, we ensure persons in day-to-day charge, nominated supervisors and FDC co-ordinators have undertaken child protection training in their state or territory (section 162A). • Our service ensures there are ongoing professional development opportunities (at induction and at regular intervals) for approved providers, educators, other staff and volunteers, to strengthen their understanding of, for example: • the service's child safe policies and procedures, Code of Conduct and Service Philosophy • identifying and responding to all forms of child maltreatment, abuse and neglect, including grooming, and how to respond through trauma informed practice • supporting a child who is disclosing child maltreatment, abuse or neglect • preventative work with families to establish and maintain child safe and culturally safe practices • responding to issues of child safety, including internal and external reporting requirements, notifying families and carers, and managing risks to children • mandatory reporting obligations • culturally safe practice, including when working with Aboriginal and Torres Strait Islander children and families. • We support educators to teach personal and online safety with children (in an appropriate way), in line with the ALFs. • We look for ways to include the voices and perspectives of children in staff training on child safety. • We invite local Aboriginal and Torres Strait Islander Elders, and community members, and culturally and linguistically diverse community members, to speak at staff meetings or service events. • Other:					
Our service does this: (select one)	Always	Mostly	Sometimes	Rarely	Never	Other (Unsure)

Self-assessment and risk assessment tool

Strengths				
Areas for improvement		Priority		
		Low	Med	High
1.				
2.				
3.				
Statement	Prompts			
b) The approved provider and service leaders support child safe practices and ensure our service's knowledge and practice remain current.	• We support educators to understand the importance of organising themselves and the service's indoor and outdoor environments to enhance supervision, including when children use digital devices and internet connected toys. • Our supervision practices minimise the need for individual educators to be alone with children. • We ensure educators understand and model positive behaviours that keep children safe and deter abuse. • We facilitate ongoing supervision and professional development of staff to encourage understanding of the importance of policies and procedures that reduce the risk of harm to children. • We provide support to staff who find themselves triggered by child safe discussions and have appropriate support mechanisms in place. • We ensure educators, staff, volunteers and students know how to raise and document concerns. • Other:			

Self-assessment and risk assessment tool

Strengths					
Areas for improvement				Priority	
		Low	Med	High	
1.					
2.					
3.					

Risk Assessment		Consider the areas for improvement. Have you identified any hazards or potential risk of harm? If yes, complete the following risk assessment to plan your response.			
		Yes	No		
Activity	Hazard/risk of harm identified	Risk assessment (use matrix)	Control measures	Who?	When?

Self-assessment and risk assessment tool

8. Complaints and disclosures

Statement	Prompts					
a) Service leaders, educators, staff and volunteers at our service respectfully respond when children make disclosures, voice a concern or complaint.	• We listen and give full attention, in a supportive and calm way, to children disclosing sensitive information. • We know to reassure the child that we believe them and that they've done the right thing by voicing their concerns. • We don't make any promises to children and let the child tell their story. We use open questions when asking children for information. • We know how to ask children making disclosures or reporting concerns what we can do to help them feel safe. • We know to inform the child of their options and what we plan to do next, which includes telling someone else who can help, and include their parent/carer in the conversation, if appropriate. • Our child safe culture considers the environment and interactions across the service, and enables children to express feelings, concerns and make complaints. • Other:					
Our service does this: (select one)	Always	Mostly	Sometimes	Rarely	Never	Other (Unsure)
Strengths						

Self-assessment and risk assessment tool

Areas for improvement	Priority		
	Low	Med	High
1.			
2.			
3.			

Statement	Prompts
b) Service leaders, educators, staff and volunteers at our service respectfully and promptly respond to complaints.	• All staff at our service understand the service's policies and procedures for responding to complaints and disclosures. • Following a disclosure or complaint, our service undertakes a risk assessment and makes a plan to act appropriately and in a timely way, to ensure children at the service are safe. • We know who to contact, and appropriate timeframes for doing so, to make a report and notify the NQF regulatory authority. • We know to ask external authorities (such as the NQF regulatory authority, police or child protection agencies) for guidance on how and when to speak to families, including families of other children at the service. • We seek support for families and/or our staff members before, during and after the complaints handling process and any investigation, and provide referrals to support organisations as needed. • Once a complaint has been addressed, we reflect on our response, learn from it, review our policies, procedures and update self-assessment and risk assessment tools where needed. • Other:

Our service does this: (select one)	Always	Mostly	Sometimes	Rarely	Never	Other (Unsure)

Self-assessment and risk assessment tool

Strengths					
Areas for improvement				Priority	
				Low	Med
1.					
2.					
3.					
Risk Assessment		Consider the areas for improvement. Have you identified any hazards or potential risk of harm? If yes, complete the following risk assessment to plan your response.			
		Yes	No		
Activity	Hazard/risk of harm identified	Risk assessment (use matrix)	Control measures	Who?	When?

Self-assessment and risk assessment tool

9. Families and communities

Statement	Prompts					
a) Service leaders, educators and staff members build strong and respectful relationships with families and talk to families about child safety concerns.	• We are open and honest with families about the service's responsibilities in creating a child safe culture, child safety obligations, and our responsibilities towards their children. • We work with families to reinforce key messages about child safety, including: • how children should be treated • teaching children to speak up if they feel unsafe • appropriate and inappropriate behaviour by adults • understanding that perpetrators may groom family members to gain access to children. • Where it is appropriate to raise a concern or issue directly with the family, we seek advice from external authorities (such as the NQF regulatory authority, police or child protection agencies) to plan: • who will speak to the family • where and when we should have the conversation • who should be present to maintain privacy and confidentiality, and • if appropriate, invite the family to bring a support person. • We consider our service's community and context and how to recognise when a child may be at increased risk, and how to have conversations about protective behaviours and keeping children safe. • Other:					
Our service does this: (select one)	Always	Mostly	Sometimes	Rarely	Never	Other (Unsure)
Strengths						

Self-assessment and risk assessment tool

Areas for improvement	Priority		
	Low	Med	High
1.			
2.			
3.			

Statement	Prompts
b) Our service engages with families to create a child safe culture and understand we prioritise the safety of children.	- We actively consult families so that we understand what makes them feel comfortable and culturally safe, and what they think will keep their children safe, happy and healthy. - We have open, two-way communication with families and communities, and consult families on the child safe practices of the service. - We work closely with families to establish and maintain child safe and culturally safe practices and to remove any barriers that would prevent families from accessing and understanding the service's policies and procedures - We take complaints seriously and have a child centred, comprehensive complaint handling system. - We ensure children, families and staff with diverse needs and family structures, including Aboriginal and Torres Strait Islander, culturally and linguistically diverse, and LGBTIQ+ families, and family members with additional needs feel included. - Other:

Our service does this: (select one)	Always	Mostly	Sometimes	Rarely	Never	Other (Unsure)
Strengths						

Self-assessment and risk assessment tool

Areas for improvement	Priority		
	Low	Med	High
1.			
2.			
3.			

Statement	Prompts
c) Our service understands the importance of building relationships with, and being connected to, families and communities.	- We support children's cultural safety and their sense of belonging by connecting them to, and engaging with, their local communities. - We engage staff, community members and Elders from the local community in committees, policy reviews and planning activities. - We invite members of diverse groups within the community to share their interests, experiences and expertise with the service. - We develop respectful connections with community members that can be used to promote child safe practices across the community. - We encourage families and the community to give feedback on child safety policies and procedures and we act on their feedback. - Other:

Our service does this: (select one)	Always	Mostly	Sometimes	Rarely	Never	Other (Unsure)

Strengths

Self-assessment and risk assessment tool

Areas for improvement		Priority		
		Low	Med	High
1.				
2.				
3.				

Risk Assessment		Consider the areas for improvement. Have you identified any hazards or potential risk of harm? If yes, complete the following risk assessment to plan your response.			
		Yes	No		
Activity	Hazard/risk of harm identified	Risk assessment (use matrix)	Control measures	Who?	When?

Self-assessment and risk assessment tool

Child Safe Culture Self-assessment and risk assessment – plan and review

Plan prepared by:

Full name:

Signature:

Role/position:
[i.e approved
provider, service
leader]

Date:

Prepared in consultation with:
(Names and roles e.g. staff, children and
families)

Next risk assessment to be conducted before

and whenever circumstances change and new child safety risks, hazards or
concerns arise.

Approved provider review

Plan reviewed by:

Full name:

Signature:

Date: