SAFE USE OF DIGITAL TECHNOLOGIES AND ONLINE ENVIRONMENTS

QUALITY AREA 7 | ELAA version 2.2

PURPOSE

This policy will provide guidelines to ensure that all users of digital technologies at Somerville Kindergarten or on behalf of Somerville Kindergarten:

- understand and follow procedures to ensure the safe and appropriate use of digital technologies Somerville Kindergarten, 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 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

VALUES

Somerville Kindergarten 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 Somerville Kindergarten. **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
- 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)*	**R**	√	√	√	√
2. Ensuring staff understand how to actively supervise children while using digital technologies	**R**	R			
3. Undertaking risk assessments *(refer to Sources)* identifying the service's digital technologies practices, identify strengths and areas for improvement	**R**	√	√		√
4. Obtaining parent/guardian consent before taking, retaining, or sharing images and videos of children *(refer to Enrolment and Orientation and Privacy and Confidentiality policy)*	R	√	√		√
5. Asking children for permission before taking photos or videos and explain how these will be used	Ö	√	√		√
6. Regularly monitoring use of service-issued electronic devices to ensure that they are being used appropriately	R	√			
7. Ensuring capturing, using, storing, and disposing of images, videos, and audio recordings of children are in line with privacy requirements *(refer to Privacy and Confidentiality policy)*	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	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.	R	R			
10. Ensuring surveillance and monitoring devices are in line with privacy requirements *(refer to CCTV policy)*	R	√			
11. Ensuring that the *Safe Use of Digital Technologies and Online Environments Policy* and procedures are implemented, the appropriate risk assessments and action plans are completed, and all identified actions are taken to minimise the risks to children's health and safety	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)	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 *(refer to Privacy and Confidentiality policy)*	R	R	√		√
14. Ensuring that person who is providing education and care and working directly with children *(refer to Definitions)* do not carry their personal electronic devices *(refer to Definitions)* while providing education and care to children, except for authorised essential purposes *(refer to Definitions)*	R	√	√	√	√
15. Ensuring authorisation is documented for when a person who is providing education and care and working directly with children *(refer to Definitions)* may need to continue to carry their personal electronic device *(refer to Definitions)* while educating and care for children (example: medical conditions) *(Refer to Attachment 6)*	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	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)	R	R	√		√
18. Providing a secure place for persons who are providing education and care, and working directly with children *(refer to Definitions),* 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	R	R	R		R

use Arrival while providing education and care and working directly with children.					
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.	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	R	R	√		√
22. Managing inappropriate use of digital technologies as described in *Attachment 2*	**R**	√			
23. Providing suitable digital technologies facilities to enable early childhood teachers, educators and staff to effectively manage and operate the service	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)	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 *(refer to Attachment 6)* documentation is completed prior to excursions and regular outings	R	R	√	√	√
26. Ensuring restricted persons *(refer to Definitions)* do not use their personal devices to record images of children when providing education and care and working directly with children	R	√	√	√	√
27. Ensuring parents/guardians do not use their personal devices to record images of children, this includes during service events	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 is issued by their business or institution; and is used only for work purposes (and not personal use)	R	√	√		√
29. Authorising the access of early childhood teachers, educators, staff, volunteers and students to the service's digital technologies facilities, as appropriate	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 *(refer to Attachment 1)*	√	√			

31. Embedding a culture of awareness and understanding of security issues at the service	**R**	√	√	√	√
32. Never posting online photos or videos of children who: • Are subject 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	**R**	√	√		√
33. 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**	√			
34. Ensuring that the service's computer software and hardware are purchased from an appropriate and reputable supplier	√	√			
35. 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	√	√			
36. Removing access on online platforms for staff, parents/guardians and others when they leave the service	R	R			
37. 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	√	√			
38. Ensuring regular backup of critical data and information at the service *(refer to Attachment 1)*	√	√	√		
39. Ensuring secure storage of all information (including images and videos of children) at the service, including backup files *(refer to Privacy and Confidentiality Policy)*	**R**	√	√		
40. Adhering to the requirements of the *Privacy and Confidentiality Policy* in relation to accessing information on the service's computer/s, including emails	**R**	**R**	**R**		
41. Considering encryption *(refer to Definitions)* of data for extra security	√	√			
42. Ensuring that reputable anti-virus and firewall software *(refer to Definitions)* are installed on service computers, and that software is kept up to date	√	√			
43. Developing procedures to minimise unauthorised access, use and disclosure of information and data, which may include limiting access, passwords, multifactor authentication and encryption *(refer to Definitions)*	**R**	√			
44. 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	**R**	√			

developing and publishing appropriate disclaimers *(refer to Definitions)*					
45. 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	**R**	√			
46. Being aware of the requirements and complying with this policy	√	√	√	√	√
47. Appropriate use of endpoint data storage devices *(refer to Definitions)* by digital technologies users at the service	**R**	√	√	√	√
48. 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	**R**	√	√		√
49. 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) *(refer to Attachment 5).*	**R**	√			√
50. Developing guidelines on the use of Artificial Intelligence (AI) *refer to Attachment 7* (if applicable to the service)	**Ö**	√			
51. Providing authorisation to early childhood teachers, educators and staff to be social media representatives for Somerville Kindergarten *(refer to Attachment 3)*	Ö	√			
52. Complying with all relevant legislation and service policies, protocols and procedures, including those outlined in *Attachments 1*	R	R	R	R	R
53. Reading and understanding what constitutes inappropriate use of digital technologies *(refer to Attachment 2)*	√	√	√	√	√
54. Ensuring that if working from home, the service device does not leave the service unless they contain no images of children *(refer to Attachment 1 and 4)*	R	R	√		√
55. Completing the authorised user agreement form when using service devices outside the service *(refer to Attachment 4)*	√	√	√		√
56. Maintaining the security of digital technologies facilities belonging to Somerville Kindergarten and keeping allocated passwords secure, including not sharing passwords and logging off after using a computer	**R**	**R**	**R**	Ö	**R**
57. Accessing accounts, data or files on the service's computers only where authorisation has been provided		√	√		√
58. Co-operating with other users of the service's digital technologies to ensure fair and equitable access to resources	√	√	√		√
59. Obtaining approval from the approved provider before purchasing licensed computer software and hardware		√	√		

60. Ensuring no illegal material is transmitted at any time via any digital technology medium *(refer to Attachment 2)*	**R**	√	√	√	√
61. Using the service's email, messaging and social media *(refer to Definitions)* facilities for service-related and lawful activities only *(refer to Attachment 2)*	√	√	√	√	√
62. Using endpoint data storage devices *(refer to Definitions)* supplied by the service for service-related business only, and ensuring that this information is protected from unauthorised access and use		√	√		√
63. Notifying the approved provider of any damage, faults or loss of endpoint data storage devices		**R**	**R**		**R**
64. 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			√	√	√
65. Signing an acknowledgement form upon receipt of a USB or portable storage device (including a laptop) *(refer to Attachment 4)*		√	√		√
66. 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	√	√	√	√	√
67. Responding only to emergency phone calls when responsible for supervising children to ensure adequate supervision of children at all times *(refer to Supervision of Children Policy)*	√	√	√		√
68. Ensuring electronic devices and files containing images and information about children and families are kept secure at all times *(refer to Privacy and Confidentiality Policy)*	**R**	**R**	**R**		**R**
69. Responding to a privacy breach in accordance with *Privacy and Confidentiality policy.*	**R**	√			
70. Complying with the appropriate use of social media *(refer to Definitions)* platforms *(refer to Attachment 3)*	√	√	√		√
71. Complying with this policy at all times to protect the privacy, confidentiality and interests of Somerville Kindergarten employees, children and families	**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.

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.

PDAs (Personal Digital Assistants): A handheld computer for managing contacts, appointments and tasks. PDAs typically include a name and address database, calendar, to-do list and note taker. Wireless PDAs 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 Somerville Kindergarten digital technology facilities:
- Attachment 6: Essential purpose authorisations
- Attachment 7: Guidelines for the use of AI

AUTHORISATION

This policy was adopted by the approved provider of Somerville Kindergarten on September 2025

REVIEW DATE: September 2026