Policy

Macedon Ranges Shire Council

Safe Use of Digital Technologies and Online Environments

Date of Adoption	24 September 2025			
Adoption Method	☐ Council	☐ CEO	☒ Director Community	
Director Signature	Signed by: Amy Holmes 819CFDCF2351437...		**Date**	26/09/2025
Responsible Officer and Unit	Samantha Waymouth, Coordinator Early Years Services			
Nominated Review Period	☐ Annually	☒ Every 4 years	☐ Other *(please specify)*	
Last Endorsement Date	New			
Next Endorsement Date	September 2029			

Macedon Ranges Shire Council acknowledges the Dja Dja Wurrung, Taungurung and Wurundjeri Woi Wurrung Peoples as the Traditional Owners and Custodians of this land and waterways. Council recognises their living cultures and ongoing connection to Country and pays respect to their Elders past, present and emerging. Council also acknowledges local Aboriginal and/or Torres Strait Islander residents of Macedon Ranges for their ongoing contribution to the diverse culture of our community.

Contents

Safe Use of Digital Technologies and Online Environments

Purpose

This policy will provide guidelines to ensure that all users of digital technologies at Macedon Ranges Shire Council Kindergartens:

- understand and follow procedures to ensure the safe and appropriate use of digital technologies, including maintaining secure storage of information
- take responsibility to protect and maintain privacy in accordance with Council's Privacy 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 and other information sharing platforms.

Values

Macedon Ranges Shire Council 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 (refer to definitions) 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 Macedon Ranges Shire Council kindergartens. This policy does not apply to children. For the use of digital technologies within their educational programs, refer to Early Years eSafety Policy.

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

- desktop top computers, laptops/notebooks, tablets, iPads, smartphones, interactive whiteboards, televisions and smart devices
- copying, saving or distributing files
- electronic mail (email)
- file sharing
- file storage (including the use of end point data storage devices)
- file transfer/Cloud
- instant messaging
- internet usage
- portable communication devices including mobile and cordless phones.
- printing material
- subscriptions to list servers, websites, mailing lists or other like services
- preschool management software and application
- video conferencing

Responsibilities

Responsibilities R indicates legislation requirement, and should not be deleted	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
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 Policy (Council), eSafety for Children and Code of Conduct Policy(Council))*	R	✓	✓	✓	✓
Ensuring staff understand how to actively supervise children while using digital technologies	R	R			
Undertaking risk assessments *(refer to references)* identifying the service's digital technologies practices, identify strengths and areas for improvement	R	✓	✓		✓
Obtaining parent/guardian consent before taking, retaining, or sharing images and videos of children *(refer to the Enrolment policy)*	R	✓	✓		✓
Asking children for permission before taking photos or videos and explain how these will be used	Ö	✓	✓		✓
Regularly monitoring use of service-issued electronic devices to ensure that they are being used appropriately	R	✓			
Ensuring capturing, using, storing, and disposing of images, videos, and audio recordings of children are in line with privacy requirements *(refer to the Privacy policy (Council))*	R	✓	✓		✓
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			
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			
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	✓		✓
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	✓	✓		✓

Ensuring the safe use of digital technologies, including wearable devices, networks, platforms, and apps, within the service	R	R	✓		✓
Ensuring that person who is providing education and care and working directly with children don't not carry their personal electronic devices while providing education and care to children, except for authorised essential purposes	R	✓	✓	✓	✓
Ensuring authorisation is documented for when a person who is providing education and care and working directly with children may need to continue to carry their personal electronic device while educating and care for children (example: medical conditions) *(Refer to Attachment 1)*	R	✓			
Ensuring a suitable log is maintained to record all essential purpose authorisation forms, that all logs are stored securely and available at the service for authorised officers to inspect	R	✓			
Maintaining a log (visitor sign in book) 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	✓		✓
Providing a secure place for persons who are providing education and care, and working directly with children, to store their personal digital devices while they are working with children	✓	✓			
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.	R	R	R		R
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.	R	R	R		R
Managing inappropriate use of digital technologies *(refer to ICT acceptable Use Policy and Procedure (Council), Mobile Device Policy and Procedure (Council) and Code of Conduct Policy (Council)*	R	✓			
Providing suitable digital technologies facilities to enable early childhood teachers, educators and staff to effectively manage and operate the service	R	✓			
Ensuring there are sufficient service-issued devices available when programs are delivered outside the approved service premises	R	R			
Ensuring staff do not use their personal devices to record images of children	R	✓			

Authorising the access of early childhood teachers, educators, staff, volunteers, parent helpers and students to the service's digital technologies facilities, as appropriate	R	R			
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 ICT acceptable Use Policy and Procedure (Council) and Mobile Device Policy and Procedure (Council)*	✓	✓			
Embedding a culture of awareness and understanding of security issues at the service	R	✓	✓	✓	✓
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	✓	✓		✓
Ensuring that the service's computer software and hardware are purchased from an appropriate and reputable supplier. All software is purchased through the Digital Technology Services department	✓	✓			
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	✓	✓			
Removing access for staff or others who leave the service	R	R			
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	✓	✓			
Ensuring regular backup of critical data and information at the service *(refer to Information Security Policy and Procedure (Council))*	✓	✓	✓		
Ensuring secure storage of all information (including images and videos of children) at the service, including backup files *(refer to Privacy Policy (Council*	R	✓	✓		
Adhering to the requirements of the *Privacy Policy (Council)* in relation to accessing information on the service's computer/s, including emails	R	R	R		
Ensuring that reputable anti-virus and firewall software are installed on service computers, and that software is kept up to date	✓	✓			
Developing procedures to minimise unauthorised access, use and disclosure of information and data, which may include limiting access, passwords, multifactor authentication and encryption	R	✓			
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 *(MRSC Cyber Incident Response Plan)*	R	✓			
Being aware of the requirements and complying with this policy	✓	✓	✓	✓	✓

Appropriate use of endpoint data storage devices by digital technologies users at the service	R	✓	✓	✓	✓
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	✓	✓		✓
Developing guidelines on the use of Artificial Intelligence (AI) *refer to IT Services for guidance (Council policy under review)*	✓	✓			
Macedon Ranges Shire Council complying with all relevant legislation and service policies, protocols and procedures.	R	R	R	R	R
Reading and understanding what constitutes inappropriate use of digital technologies *(refer to ICT acceptable Use Policy and Procedure (Council), Mobile Device Policy and Procedure (Council) and Code of Conduct Policy (Council)*	✓	✓	✓	✓	✓
Maintaining the security of digital technologies facilities belonging to and keeping allocated passwords secure, including not sharing passwords and logging off after using a computer	R	R	R	Ö	R
Accessing accounts, data or files on the service's computers only where authorisation has been provided		✓	✓		✓
Obtaining approval from the IT department before purchasing licensed computer software and hardware		✓	✓		
Ensuring no illegal material is transmitted at any time via any digital technology medium *(refer to ICT acceptable Use Policy and Procedure (Council), Mobile Device Policy and Procedure (Council) and Code of Conduct Policy (Council)*	R	✓	✓	✓	✓
Using the service's email, and online platform for service-related and lawful activities only *(refer to ICT acceptable Use Policy and Procedure (Council), Mobile Device Policy and Procedure (Council) and Code of Conduct Policy (Council)*	✓	✓	✓	✓	✓
Notifying the approved provider of any damage, faults or loss of endpoint data storage devices		R	R		R
Notifying the approved provider, nominated supervisor, and/or Regional Team Leader immediately if they observe any inappropriate use of personal or service issued electronic devices at the service			✓	✓	✓
Responding only to emergency phone calls when responsible for supervising children to ensure adequate supervision of children at all times *(refer to Early Years Supervision of Children Policy)*	✓	✓	✓		✓
Ensuring electronic devices and files containing images and information about children and families are kept secure at all times *(refer to Privacy Policy (Council))*	R	R	R		R
Responding to a privacy breach in accordance with *Privacy policy (Council).*	R	✓			
Complying with this policy at all times to protect the privacy, confidentiality and interests of employees, children and families	R	R	R		R

Background/Reasons for Policy

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, enabling hackers to access Wi-Fi networks, track device locations, and potentially use audio and video functions poses 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 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.

Gender Impact Assessment

In accordance with the Gender Equality Act 2020, a Gender Impact Assessment was not required in relation to the subject matter of this report.

Definitions

Term	Definition
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.
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.
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: • an emergency situation 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, e.g. heart or blood sugar level monitoring • disability-related communication needs (essential means of communication) • family necessity (e.g. seriously ill immediate family member) • technology failure (e.g. outage of service-issued devices) • local emergency event (e.g. bushfire notification) • emergency communication during excursions and regular outings (e.g. if a group is split up and you do not have two kindergarten devices) • emergency communication when children are transported or travel on transport arranged by the service.
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.
Information sharing platforms	Describes the exchange of data between various organisations, people and technologies This can include but no limited to SharePoint, One Drive.
Illegal material	Illegal material 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.
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.
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.
USB /Flash drive	Also known as sticks, drives, memory keys and flash drives, a USB is a device that plugs into the computer's USB port and is small enough to hook onto a key ring. A USB allows data to be easily downloaded and transported/transferred.

References

- 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

- Early Years Child Safe Environment and Wellbeing
- Code of Conduct (Council)
- Complaints (Council)
- Early Years Educational Program
- Early Years Enrolment

- Early Years eSafety for Children
- Early Years Governance and Management of the Service
- Occupational Health and Safety (Council)
- Privacy (Council)
- Early Years Staffing
- ICT Acceptable Use Policy and Procedure (Council)
- Mobile Device Policy and Procedure (Council)
- Information Security Policy and Procedure (Council)
- Cyber Incident Response Plan (Council)

Related Legislation

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)
- Trade Marks Act 1995 (Cth)

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: Early Years Staff – Personal Device Exemptions form
- Attachment 2: Staff procedure for personal devices