SAFE USE OF DIGITAL TECHNOLOGIES AND ONLINE ENVIRONMENTS POLICY

QUALITY AREA 2 – VERSION 2.3

PURPOSE

This policy provides guidelines to ensure that all users of digital technologies at, or on behalf of, Denzil Don Kindergarten:

- Understand and follow procedures that support the safe and appropriate use of digital technologies at the service, including maintaining the secure storage of information
- Take all reasonable steps to protect and maintain privacy in accordance with the service's Privacy and Confidentiality Policy
- Promote a child-safe culture in relation to the taking, use, storage, and destruction of images of children
- Are aware that only individuals authorised by the Approved Provider are permitted access to digital devices at the service
- Understand what constitutes illegal or inappropriate use of digital technologies and actively avoid such activities
- Use interactive digital platforms and other information-sharing tools, in a professional, safe and appropriate way.

POLICY STATEMENT

The safety, health, wellbeing, rights and best interests of every child guide all decisions, actions and practices of Denzil Don Kindergarten staff.

VALUES

Denzil Don Kindergarten is committed to:

- Providing a safe environment through the creation and maintenance of a child-safe culture. This includes ensuring the safe, respectful and appropriate use of digital technologies and online environments.
- Promoting professional, ethical and responsible use of digital technologies by all staff, volunteers and visitors.
- Maintaining a safe and supportive workplace for all staff in their use of the service's digital technologies, communication systems and information-sharing platforms.
- Upholding the rights of all children to feel safe and be safe at all times, including digitally.
- Safeguarding the privacy, confidentiality and security of all information that is received, transmitted or stored electronically, in accordance with relevant privacy laws and best practices.
- Ensuring that all use of digital technologies aligns with service policies, procedures and applicable government legislation, including child safety, privacy and data protection requirements.
- Providing all staff with access to appropriate online information, resources and communication tools to support the effective, efficient and compliant operation of the service.

SCOPE

This policy applies to the Approved Provider, all service staff (educational and non-educational), students, volunteers, parents/carers, and others attending the programs and activities of Denzil Don Kindergarten. **This policy does not apply to children.**

Parent/Carer Responsibilities Under This Policy:
Never take photographs, videos, or audio recordings of children at the service, including during excursions, regular outings, or service events
Comply with rules about personal devices at the service
Comply with all service procedures, and protocols relating to digital technology use
Read, understand and follow the service Code of Conduct at all times
Adhere to this policy and all other service policies at all times

Responsibilities: **R** indicates legislation requirement	Approved provider & persons with management or control	Nominated Supervisor and Person in Day-to-Day Charge	All service staff (educational & non-educational)	Contractors, Volunteers & Students
Ensure that the use of the service's digital technologies complies with all relevant state and federal legislation and service policy *(including Privacy and Confidentiality, eSafety for Children, Code of Conduct)* (Standard 2)	**R**	√	√	√
Avoid inappropriate conduct and always maintain professional boundaries with children, and behave in line with the *Code of Conduct, Child Safe Environment and Wellbeing Policy & Interaction with Children Policy* (Standard 2)	**R**	**R**	**R**	**R**
Follow this policy and all service policies, to protect privacy, confidentiality and the interests of the service, children and families (Standard 2,9)	**R**	**R**	**R**	**R**
Comply with legislation, policies and procedures (Standard 2)	**R**	**R**	**R**	**R**
Obtain parent/carer consent before taking, retaining, or sharing images of children *(see Enrolment and Orientation and Privacy and Confidentiality Policy)* (Standard 4,9)	**R**	√	√	√
Ensure capture, use, storage, and disposal of images, videos, and audio recordings of children align with privacy requirements *(see Privacy and Confidentiality Policy)* (Standard 2,9)	**R**	√	√	√
Ensure oversight and control over who has access to images of children, including movement across devices and platforms (Standard 2,9)	**R**	**R**		
Ensure staff do not transfer images of children to personal accounts or devices, including via cloud services (Standard 2,9)	**R**	**R**		
Ensure devices used offsite contain no child images (Standard 2)	**R**	**R**	√	√
Respond to privacy breaches according to the *Privacy and Confidentiality Policy* (Standard 2)	**R**	√		
Develop procedures to prevent unauthorised access, use, or disclosure of data (Standard 2)	**R**	√		
Ensure secure storage of all information, including backups *(refer to Privacy and Confidentiality Policy)* (Standard 2)	**R**	√		
Keep devices and files containing child information secure	**R**	**R**	**R**	**R**
Store all data on secure backup systems (Standard 2)	**R**	√	√	√
Maintain system security, including password protection	**R**	**R**	**R**	**R**
Remove access to systems when staff or families leave the service	**R**	**R**		
Ensure no illegal material transmits via service systems	**R**	√	√	√
Embed awareness of cyber security and safety issues (Standard 2)	**R**	√	√	√
Ensure secure financial processes for digital transactions	**R**	√		
Limit liability through appropriate disclaimers (Standard 2)	**R**	√		
Use laptops and other service owned digital devices for work only and protect data		√	√	√
Use laptops and other service devices appropriately (Standard 2)	**R**	√	√	√
Ensure adequate service-issued devices for offsite programs (Standard 9)	**R**	**R**	**R**	**R**
Ensure safe use of digital technologies (including wearable devices) in line with privacy principles (Standard 2,9)	**R**	**R**	√	√

Report damage, faults or loss of devices to the Centre Coordinator immediately		R	R	R
Provide suitable digital technologies to support service operations (Standard 2,9)	R	√		
Ensure persons providing education and care do not carry personal electronic devices while working directly with children, except for authorised essential purposes (Standard 9)	R	√	√	√
Ensure educators do not use personal devices for multi-factor authentication while working directly with children (Standard 2,9)	R	R	R	R
Ensure access to personal devices occurs only when not working directly with children (Standard 9)	R	R	R	R
Provide secure storage for personal devices while staff work with children	√	√	√	√
Ensure documentation of authorisation where a person requires access to a personal device while working with children (e.g. medical needs) (Standard 2,9)	R	√		
Maintain a secure log of all essential purpose authorisations for inspection by authorised officers (Standard 2)	R	√		
Ensure staff understand how to actively supervise children while using digital technologies (Standard 8,9)	R	R		
Respond only to emergency calls while supervising children, and request another staff member to step in to the classroom so you can do so *(see Supervision of Children Policy)*	√	√	√	√
Promote a culture of child safety and wellbeing across all service operations, including online environments (Standard 2,9)	R	√	√	√
Ensure implementation of the *Safe Use of Digital Technologies* and *Online Environments Policy*, completion of risk assessments, and action to minimise risks to children (Standard 2,9)	R	R	√	√
Conduct risk assessments to identify the service's digital technology practices, strengths and areas for improvement (Standard 2,9)	R	√	√	√
Undertake risk assessments to ascertain if personal devices can be used at the service, and in what circumstances (including wearables) (Standard 2,9)	R	R	√	√
Ensure third-party professionals use only organisation-issued devices for work purposes (Standard 9)	R	√	√	√
Maintain a log for third-party professionals (such as Allied Health) who use organisation-issued devices for work purposes only (Standard 2,9)	R	R	√	√
Obtain parent permission for system access by persons under 18 (e.g. students on placement) (Standard 2)	R	√		√
Ensure restricted persons and parents/carers do not use personal devices to record images of children (Standard 9)	R	√	√	√
Ensure personal devices with cameras are used only in emergencies during excursions and with prior authorisation (Standard 2,9)	R	R	√	√
Authorise access to service digital technologies for staff and others as appropriate (Standard 2,9)	R	R		
Provide clear procedures for use of digital technologies onsite and when working from home (Standard 2,9)	√	√		
Use communication platforms for work-related purposes only	√	√	√	√
Monitor use of service-issued electronic devices to ensure appropriate use, and ensure any inappropriate use is managed appropriately (Standard 2,7, 9)	R	√		
Report any observations of inappropriate use of personal or service issued electronic devices at the service to the Centre Coordinator (Standard 2)		√	√	√

BACKGROUND & LEGISLATION

BACKGROUND

The digital technology landscape is constantly evolving, with early childhood services increasingly using digital devices to support research, communication, and service management. While digital technology provides efficiency, they also introduce significant legal and ethical responsibilities regarding information privacy, security, and the protection of service staff, families, and 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 breaches of privacy), 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 (VECRA) requires approved providers and service management to comply with the National Model Code. This Code is crucial for ensuring the safety and privacy of children. At Denzil Don Kindergarten, in accordance with the Code, only service-issued electronic devices are used to take photographs of children, minimising the risk of unauthorised distribution of images. Personal devices are not permitted in classrooms at any time. This applies to service staff, families, and those working in partnership with the service (including Allied Health professionals and PSFOs).

Denzil Don Kindergarten does not share identifiable images of children online. Images shared in the Journal are blurred or limited to non-identifiable shots, such as hands or the back of the head. Video and audio recordings of children are never taken. Denzil Don Kindergarten also does not participate in social media.

LEGISLATION & 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, see the Definitions File located online: https://denzildonkinder.org.au/policies/ OR in the Policies Folder in the kindergarten office.

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.

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 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.
- 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.

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, and or footage of real violence, cruelty and criminal activity.

Inappropriate conduct: Conduct that a reasonable person would consider inappropriate in an education and care service, considering 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 with words or behaviour, including both adult to child or between adults in a child's presence
- filming and capturing images or recordings
- as a single occasion or as part of a pattern over time
- either directly or indirectly (eg: exposure to inappropriate language or leaving inappropriate material accessible to children)
- online
- as an omission (for example, deliberately excluding a child).

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. 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 workplace and used only for work purposes (and not personal use).

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

Digital literacy: the ability to identify and use technology confidently, creatively, and safely.

eSafety Commissioner: Australia's national independent regulator for online safety. purpose is to help safeguard Australians at risk from online harms and to promote safer, more positive online experiences

SOURCES & RELATED POLICIES

SOURCES

- Department of Education resources

- 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: How do I manage a data breach?

RELATED POLICIES

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

EVALUATION

To assess whether the values and purposes of the policy have been achieved, we will:

- seek feedback from all parties 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
- notify all stakeholders affected by this policy at least 14 days before any significant change is made to the policy or its procedures, unless a lesser period is necessary due to risk *(Regulation 172 (2))*.

PROCEDURES

- Procedure 1: Use of Digital Technology at the Service
- Procedure 2: Unacceptable and Inappropriate Use of Digital Technology

ATTACHMENTS

- NIL

AUTHORISATIONS

This policy was adopted by the approved provider of Denzil Don Kindergarten on 19/06/2026.

REVIEW DATE: **19 June 2028**

PROCEDURE 1: UNACCEPTABLE AND INAPPROPRIATE USE OF DIGITAL TECHNOLOGY

Prohibited Use of Digital Technology

Users of digital technology facilities provided by the service must not:

- Create, access, or exchange messages that are offensive, harassing, obscene, or threatening.
- Use digital technology facilities to gain unauthorised access to other systems or networks.
- Engage in illegal, inappropriate, or offensive activities, including but not limited to hate speech or content that discriminates on the basis of race, nationality, religion, disability, gender, or sexual orientation.
- Access, download, create, store, or distribute illegal, offensive, obscene, or objectionable material, including pornography or sexually explicit material. Consent of recipients does not make such use acceptable.
- Use digital technology to send personal communications that may imply they are acting in an official capacity on behalf of the service.
- Conduct outside business activities or employment-related work for another organisation using the service's digital systems.
- Use digital technology facilities for non-work-related entertainment purposes.
- Share or exchange confidential or sensitive information without proper authorisation.
- Harass, intimidate, defame, vilify, threaten, or otherwise harm individuals or groups.
- Breach copyright laws by copying, downloading, or distributing protected material without permission.

Management of Breaches

- Service staff or other individuals in partnership with Denzil Don Kindergarten who use digital technologies for unlawful purposes may be subject to criminal or civil legal action, including fines, damages, or imprisonment. The approved provider will not support or defend unlawful actions.
- The service reserves the right to block access to internet sites where inappropriate use is identified.
- Staff who breach this procedure may be subject to counselling, disciplinary action, or termination of employment.
- All service staff, volunteers, and students who do not comply may have access to digital technology facilities restricted or removed.

Categories of Inappropriate Use

Category 1: Illegal – Criminal Use of Material

This includes, but is not limited to:

- Child abuse material offences as defined under the Crimes Act 1958 (Vic).
- Accessing or distributing objectionable material classified as X18+ or Refused Classification (RC) under classification legislation.
- Reckless or deliberate copyright infringement or any activity that breaches criminal law.

Category 2: Extreme – Non-Criminal Use of Material

This includes material that may be classified as RC or X18+, including content that:

- Depicts sex, drug misuse, crime, cruelty, or violence in a way that is offensive to community standards.
- Depicts or describes a person under 18 in a way likely to offend a reasonable adult.
- Promotes, incites, or instructs in criminal or violent behaviour.
- Contains explicit sexual activity between consenting adults.

Category 3: Critical – Offensive Material

This includes material that:

- May be classified as R18+ (high-impact content, including sex scenes or drug use).
- Includes sexualised nudity.
- Promotes racial or religious vilification.
- Is discriminatory or defamatory.
- Involves bullying or sexual harassment.

Category 4: Serious – Improper Use

- Includes any use of digital technology that is offensive, inappropriate, or inconsistent with service values.
- This category applies to behaviours not specifically outlined above but deemed unacceptable based on circumstances and context.

Additional Considerations

- These categories are not exhaustive. Any breaches not specifically listed will be assessed on a case-by-case basis, considering the nature, severity, and impact of the conduct.

PROCEDURE 2: USE OF DIGITAL TECHNOLOGIES AT THE SERVICE

Digital Storage of Personal and Health Information

- All digital records containing personal, sensitive, or health information, including images of children, is stored digitally on Teams, with password-protected to maintain privacy and confidentiality.
- Hardcopy enrolment records can only be taken off the service premises with authorisation from the Cenre Coordinator and/or Educational Leader (see Privacy and Confidentiality Policy).
- Unauthorised access to information or modification of data is strictly prohibited.

Working From Home Procedure

When working remotely, all staff must:

- Complete an Authorised User Agreement Form (digital).
- Ensure that images of children are not accessed, stored, or transferred onto personal devices.
- Maintain confidentiality and security of all work materials, including personal, sensitive, and health information, as well as planning and children's records.
- Comply with the Privacy and Confidentiality Policy.
- Report any actual or suspected breaches of privacy, or loss of personal, sensitive, or health information to the nominated supervisor or approved provider as soon as practicable.