INFORMATION & COMMUNICATION TECHNOLOGY

QUALITY AREA 7 | ELAA version 1.2

PURPOSE

This policy will provide guidelines to ensure that all users of information and communication technology (ICT) at Denzil Don Kindergarten or on behalf of Denzil Don Kindergarten:

- understand and follow procedures to ensure the safe and appropriate use of ICT Denzil Don Kindergarten, including maintaining secure storage of information.
- take responsibility to protect and maintain privacy in accordance with the service's *Privacy and Confidentiality Policy*
- are aware that only those persons authorised by the approved provider are permitted to access ICT at the service.
- understand what constitutes illegal and inappropriate use of ICT facilities and avoid such activities.
- understand and follow professional use of interactive ICT platforms, such as social media *(refer to Definitions)* and other information-sharing platforms *(refer to Definitions).*

POLICY STATEMENT

VALUES

Denzil Don Kindergarten is committed to:

- professional, ethical, and responsible use of ICT.
- providing a safe workplace fo all staff and volunteers using service ICT facilities and information-sharing platforms
- safeguarding the privacy and confidentiality of electronic information.
- ensuring the use of ICT at the service complies with policies and government legislation.
- providing all staff with online information, resources, and communication tools to support the effective operation of the service.

SCOPE

This policy applies to staff, students, volunteers, visitors, parents/carers, and others attending programs and activities at Denzil Don Kindergarten. **This policy does not apply to children**. This policy applies to all aspects of the use of ICT.

RESPONSIBILITIES	Approved provider and persons with management or control	Nominated supervisor and persons in day-to-day charge	All staff including teaching and non-teaching	Parents/carers	Contractors, volunteers and students
R indicates legislation requirement and should not be deleted					

Ensuring that the use of the service's ICT complies with all relevant state and federal legislation *(refer to Legislation and standards),* and all service policies *(including Privacy and Confidentiality Policy and Code of Conduct Policy)*	**R**	√	√	√	√
Managing inappropriate use of ICT as described in *Attachment 2*	**R**	√			
Providing suitable ICT facilities to enable all early childhood staff to effectively manage and operate the service	√	√			
Ensuring staff do not use their personal devices to record images of children *(National Law 167)*	R	R			
Authorising the access of early childhood staff, volunteers, and students to the service's ICT facilities, as appropriate	√	√			
Providing clear procedures and protocols that outline the parameters for use of the service's ICT facilities both at the service and when working from home *(refer to Attachment 1)*	√	√			
Embedding a culture of awareness and understanding of security issues at the service	**R**	√	√	√	√
Ensuring that effective financial procedures and security measures are implemented where transactions are made using the service's ICT facilities, e.g. invoice payments, and using online banking	**R**	√			
Ensuring that the service's computer software and hardware are purchased from an appropriate and reputable supplier	√	√			
Identifying the need for additional password-protected email accounts for early childhood staff, and others at the service, and providing these as appropriate	√	√			
Identifying the training needs of early childhood staff in relation to ICT, and providing recommendations for the inclusion of training in ICT in professional development activities	√	√			
Ensuring regular backup of critical data and information at the service *(refer to Attachment 1)*	√	√	√		
Ensuring secure storage of all information at the service, including backup files *(refer to Privacy and Confidentiality Policy)*	**R**	√	√		
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**		
Considering encryption *(refer to Definitions)* of data for extra security	√	√			
Ensuring that reputable anti-virus and firewall software *(refer to Definitions)* 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 and passwords, and encryption *(refer to Definitions)*	**R**	√			
Ensuring that the service's liability in the event of security breaches or unauthorised access, use, and disclosure of	**R**	√			

information and data is limited by developing and publishing appropriate disclaimers *(refer to Definitions)*					
Developing procedures to ensure data and information (e.g. passwords) are kept secure and only disclosed to individuals where necessary	**R**	√			
Being aware of the requirements and complying with this policy	√	√	√	√	√
Appropriate use of endpoint data storage devices *(refer to Definitions)* by ICT users at the service	**R**	√	√	√	√
Ensuring that all material stored 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**	√	√		√
Ensuring that written permission is provided by parents/carers 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**	√			√
Complying with all relevant legislation and service policies, protocols, and procedures, including those outlined in *Attachments 1*	√	√	√	√	√
Reading and understanding what constitutes inappropriate use of ICT *(refer to Attachment 2)*	√	√	√	√	√
Completing the authorised user agreement form *(refer to Attachment 4)*	√	√	√		√
Maintaining the security of ICT facilities belonging to Denzil Don Kindergarten and keeping allocated passwords secure, including not sharing passwords and logging off after using a computer	**R**	**R**	**R**	√	**R**
Accessing accounts, data, or files on the service's computers only where authorisation has been provided		√	√		√
Co-operating with other users of the service's ICT to ensure fair and equitable access to resources	√	√	√		√
Ensuring no illegal material is transmitted at any time via any ICT medium *(refer to Attachment 2)*	**R**	√	√	√	√
Using the service's email and other online services *(refer to Definitions)* for service-related and lawful activities only *(refer to Attachment 2)*	√	√	√	√	√
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		√	√		√
Notifying the approved provider of any damage, faults, or loss of endpoint data storage devices		**R**	**R**		**R**
Signing an acknowledgment form upon receipt of a portable storage device (including a laptop) *(refer to Attachment 4)*		√	√		√
Restricting the use of personal mobile phones to rostered breaks and only in areas outside of spaces being utilised for education and care of children	√	√	√	√	√
Advising family and friends that emergency phone calls must be made to the service landline to ensure that supervision of	√	√	√		√

children is maintained at all times *(refer to Supervision of Children Policy)*					
Ensuring electronic files containing information about children and families are always kept secure *(refer to Privacy and Confidentiality Policy)*	R	R	R		R
Responding to a privacy breach in accordance with *Privacy and Confidentiality policy.*	R	√			
Complying with this policy at all times to protect the privacy, confidentiality and interests of Denzil Don Kindergarten employees, children and families	R	R	R		R

PROCEDURES

Refer to *Attachment 1* for the following procedures including email usage, digital storage of personal and health information, and password management.

BACKGROUND AND LEGISLATION

BACKGROUND

The ICT environment is continually changing. Early childhood services now have access to a wide variety of technologies. While ICT is a cost-effective, timely, and efficient tool for research, communication, and management of a service, there are also legal responsibilities in relation to information privacy, security, and the protection of employees, families, and children.

State and federal laws, including those governing information privacy, copyright, occupational health and safety, anti-discrimination, and sexual harassment, apply to the use of ICT *(refer to Legislation and standards).* Illegal and inappropriate use of ICT resources includes pornography, fraud, defamation, breach of copyright, unlawful discrimination or vilification, harassment (including sexual harassment, stalking, and privacy violations) and privacy violations), and illegal activity, including illegal peer-to-peer file sharing.

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. Refer to the definitions file on the kindergarten website for regularly used terms.

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 the 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 seek 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: 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 similar, cameras with USB drive connection, iPhones/smartphones, PCI/PC Card/PCMCIA storage cards, and PDAs (Personal Digital Assistants).

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.

Information sharing platforms: Describes the exchange of data between various organisations, people, and technologies. This includes Dropbox, Google Drive, Sharepoint, Skype, One Drive

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.

Phishing: 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 can store and transfer large volumes of data. Devices are either used for data storage (for example, USB keys) or multiple other functions (such as iPods and PDAs).

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

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

Social Media: Denzil Don Kindergarten does not use social media.

Spam: unsolicited and unwanted emails or other electronic communication.

USB key: a device that plugs into the computer's USB port to download and transfer data.

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.

SOURCES AND RELATED POLICIES

SOURCES

- Acceptable Use Policy, DE Information, Communications and Technology (ICT) Resources: https://www.education.vic.gov.au/school/teachers/management/infrastructure/Pages/acceptableuse.aspx
- IT for Kindergartens: www.kindergarten.vic.gov.au

RELATED POLICIES

- Code of Conduct
- Compliments and Complaints
- Educational Program
- Enrolment and Orientation
- eSafety for Children
- 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, the service will:

- 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 policy review cycle or as required.

- notify stakeholders affected by this policy at least 14 days before making significant changes to it or its procedures, unless a lesser period is necessary due to risk *(Regulation 172 (2))*

ATTACHMENTS

- Attachment 1: Procedures for use of ICT at the service
- Attachment 2: Unacceptable/inappropriate use of ICT facilities
- Attachment 3: Social Media Guidelines
- Attachment 4: Authorised user agreement (online document)

AUTHORISATION

This policy was adopted by the approved provider of Denzil Don Kindergarten on 21/12/2023.

REVIEW DATE: 21 / DECEMBER / 2025

ATTACHMENT 1. PROCEDURES FOR USE OF ICT AT THE SERVICE

Email usage

- Create an email signature that identifies the employee's name, title, service name, and service phone number.
- Always include a disclaimer *(refer to Definitions),* 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.
- Be suspicious of phishing titles.

Digital storage of personal and health information

- Digital records containing personal, sensitive, and/or health information or photographs of children must be password-protected and stored securely so that privacy and confidentiality are 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 photographs 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)*. In such circumstances, services must ensure that the information is transported, handled, and stored securely so that privacy and confidentiality are always maintained.
- ICT users are not to view or interfere with other users' files or directories, knowingly obtain unauthorised access to information or damage, delete, or otherwise alter data without permission.
- Ensure all material stored on an endpoint data storage device is backed up to the cloud.

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 as part of the overall security strategy. The technical considerations and principles outlined below are intended to be used as a guide for developing a password procedure.

Users should always follow these principles:

- do not share passwords with anyone.
- never use the same password for work accounts as the one you have for personal use.
- 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 a staff member works from home, they must:

- complete the authorised user agreement form *(refer to Attachment 4)*
- ensure security and confidentiality of workspace, keeping private, sensitive health information, planning, educational programs, and children's records confidential and secure always.
- keep allocated passwords secure, including not sharing passwords and logging off after using a computer.
- adhere to the *Privacy and Confidently Policy*
- report breaches to privacy or loss of private, sensitive, and health information to nominated superiors as soon as possible.

ATTACHMENT 2. UNACCEPTABLE/INAPPROPRIATE USE OF ICT FACILITIES

Users of the ICT facilities provided by Denzil Don Kindergarten must not:

- carry out illegal, inappropriate, or offensive activities to fellow employees or the public. Such activities include but are not limited to, hate speech or material that ridicules/discriminates against others based on race, nationality, creed, religion, ability/disability, gender, or sexual orientation.
- use the ICT 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 ICT 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 Denzil Don Kindergarten
- play games.
- exchange any confidential or sensitive information held by Denzil Don Kindergarten unless authorised.
- harass, slander, intimidate, embarrass, defame, vilify, seek to offend, or make threats against another person or group of people.
- breach copyright laws by making copies of or transmitting material or commercial software.
- send Denzil Don Kindergarten property to a personal email address. This includes forwarding work correspondence and sending files and documents that Denzil Don Kindergarten owns or are owned by a Denzil Don Kindergarten employee. This includes child and/or family records such as enrolment paperwork, medical information etc.

Breaches of this policy

- Individuals who use ICT 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 ICT facilities for an unlawful purpose.
- Employees who fail to adhere to this policy may be liable to counselling, disciplinary action or dismissal.
- Service staff, volunteers, and students who fail to adhere to this policy may have their access to the service's ICT 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 offend 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-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

Denzil Don Kindergarten does not use social media to communicate with families.

The below directives are essential to the safety and wellbeing of staff, children, and their families and to ensure that Denzil Don Kindergarten operates in a professional and appropriate manner when using information-sharing platforms.

Staff must exercise extreme caution using ICT facilities when accessing information-sharing platforms, whether in the workplace or relating to external events or functions involving Denzil Don Kindergarten.

It is a breach of confidentiality and privacy to make posts or comments about children, families, staff, or management from Denzil Don Kindergarten 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.

Denzil Don Kindergarten specifically requires that, unless you have permission, you:

- Do not video or photograph anyone or post photos or personal details of other Denzil Don Kindergarten staff, children, or families.
- Do not post photos or videos of Denzil Don Kindergarten staff, children, or families on your personal social media page or otherwise share photos or videos of staff, children, or families through social media.
- Do not create a Denzil Don Kindergarten branded social media page or other pages or content on social media that represents Denzil Don Kindergarten, its staff, children, or families without authorisation from the approved provider.
- Do not post anything that could embarrass or damage the reputation of Denzil Don Kindergarten, 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 Denzil Don Kindergarten reputation or bring it into disrepute.
- imply that they are authorised to speak as a representative of Denzil Don Kindergarten or give the impression that the views expressed are those of Denzil Don Kindergarten unless authorised to do so
- use a Denzil Don Kindergarten email address or any Denzil Don Kindergarten 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 Denzil Don Kindergarten;
- use or disclose any confidential information or personal information obtained in the capacity as an employee/contractor of Denzil Don Kindergarten or
- access and/or post on personal social media during paid work hours.

Personal use of social media

Denzil Don Kindergarten 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 Denzil Don Kindergarten that can occur through their use of social media, even if their activity occurs outside working hours or on devices not owned by Denzil Don Kindergarten.

If an individual can be identified as an employee of Denzil Don Kindergarten 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 Denzil Don Kindergarten
- expressly state on all postings (identifying them as an employee of Denzil Don Kindergarten) the stated views are their own and are not those of Denzil Don Kindergarten.
- 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 that breach Denzil Don Kindergarten 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 the unacceptable use of social media as described above.

Consequences of unacceptable use of social media

- Denzil Don Kindergarten will review any alleged breach of this policy on an individual basis. If the alleged breach is serious, the person shall be given an opportunity to be heard in relation to the breach.
- If the alleged breach is 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 Denzil Don Kindergarten *Code of Conduct Policy*.
- Denzil Don Kindergarten may request that any information contained on any social media platform that breaches this policy be removed.
- Denzil Don Kindergarten may restrict an employee's access to social media on ICT facilities or if they have breached this policy, while Denzil Don Kindergarten investigates whether they have breached this policy.

ATTACHMENT 4. AUTHORISED USER AGREEMENT (ONLINE DOCUMENT)

Laptop

I, ____ ,

- acknowledge that I have received a laptop belonging to Denzil Don Kindergarten
- will ensure that the laptop:
  - is used for work-related purposes only
  - is password-protected at all times
  - will not be loaned to unauthorised persons
  - will be returned to Denzil Don Kindergarten on cessation of employment
- will notify the Centre Coordinator as soon as is practicable if the laptop is damaged, faulty, or lost
- have read the Denzil Don Kindergarten Information and Communication (ICT) Technology Policy and agree to abide by the procedures outlined.

______________________________ ______________________________

Signature (authorised user) Position

____

Date

______________________________ ______________________________

Authorised by Position

____

Date