INFORMATION & COMMUNICATION TECHNOLOGY

QUALITY AREA 7 | ELAA version 1.0

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

PURPOSE

This policy provides guidelines for users of information and communication technology (ICT) at Denzil Don Kindergarten, or on behalf of Denzil Don Kindergarten, to ensure they:

- understand and follow procedures to ensure the safe and appropriate use of technology at 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 at the service
- providing a safe workplace for management, educators, staff and others using the service's ICT facilities and information sharing platforms
- safeguarding the privacy and confidentiality of information received, transmitted or stored electronically
- ensuring that the use of the service's technology device(s) 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 Denzil Don Kindergarten. **This policy does not apply to children**.

This policy applies to all aspects of the use of technology including computers (desktop, laptops, tablets, iPads, smartphones), copying, saving, sharing or distributing files, email, storage (including the use of end point data storage devices – *refer to Definitions*) and transfer, instant messaging, internet usage, online discussion groups and chat facilities, mobile and cordless phones, printing, social media *(refer to Definitions),* streaming media, subscriptions to list servers, mailing lists or other like services, video conferencing and viewing material electronically.

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
Ensuring that the use of the service technology 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)*	√	√	√	√	√
Managing inappropriate use of technology as described in *Attachment 2*	√	√			
Providing appropriate technology to enable early childhood teachers, educators and staff to effectively manage and operate the service	√	√			
Authorising the access of early childhood teachers, educators, staff, volunteers and students to the service's ICT facilities, as appropriate	√	√			
Providing clear procedures and protocols that outline the parameters for use of technology 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	√	√	√		
Ensuring that effective financial procedures and security measures are implemented where transactions are made using the technology, e.g. handling fees, and online banking	√	√			
Ensuring that the service's computer software and hardware are purchased from an appropriate and reputable supplier	√	√			
Identifying the need for password-protected email accounts for management, early childhood teachers, educators, staff and others at the service, and providing them as appropriate	√	√			
Identifying technology training needs of early childhood teachers, educators and staff and offering recommendations for the inclusion of technology training in professional development	√	√			
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)*	√	√	√		
Adhering to the requirements of the *Privacy and Confidentiality Policy* in relation to accessing information on the service's computer/s, including emails	√	√	√		

Ensuring reputable anti-virus and firewall software *(refer to Definitions)* is 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, and encryption *(refer to Definitions)*	√	√			
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 *(refer to Definitions)*	√	√			
Developing procedures to ensure data and information are kept secure, and only disclosed to individuals where necessary	√	√			
Being aware of the requirements and complying with this policy	√	√	√	√	√
Appropriate use of endpoint data storage devices *(refer to Definitions)* by technology users at the service	√	√	√	√	√
Ensuring that all material stored on endpoint data storage devices is backed up and that devices are stored securely	√	√	√		√
Providing authorisation to early childhood teachers, educators and staff to be social media representatives for Denzil Don Kindergarten *(refer to Attachment 3)*	√	√			
Complying with all relevant legislation and service policies, protocols and procedures, including those outlined in *Attachment 1*	√	√	√	√	√
Reading and understanding what constitutes inappropriate use of technology *(refer to Attachment 2)*	√	√	√	√	√
Completing the authorised user agreement form *(refer to Attachment 4)*	√	√	√		√
Maintaining the security of technology belonging to Denzil Don Kindergarten and keeping allocated passwords secure, including not sharing passwords and logging off after using a computer	√	√	√	√	√
Accessing accounts, data or files on the service's computers only where authorisation has been provided		√	√		√
Co-operating with other users of service technology to ensure fair and equitable access to resources	√	√	√		√
Obtaining approval from the approved provider before purchasing licensed computer software and hardware		√	√		
Ensuring no illegal material is transmitted at any time via any technology device *(refer to Attachment 2)*	√	√	√	√	√
Using the service's email and social media *(refer to Definitions)* for service-related and lawful activities only *(refer to Attachment 2)*	√	√	√	√	√
Using service-supplied endpoint data storage devices *(refer to Definitions)* for service-related operations only, and ensuring this information is protected from unauthorised access and use		√	√		√
Notifying the Centre Coordinator of any damage, faults or loss of endpoint data storage devices		√	√		√

Signing an acknowledgement form upon receipt of a Denzil Don Kindergarten laptop *(refer to Attachment 4)*		√	√		√
Restricting the use of personal mobile phones to work related activities (eg: photographs for reflections/observations) and ensuring photographs of children are downloaded to a password protected service device and then deleted from the mobile after session and at the latest, prior to departing the service premises	√	√	√		√
Restricting the use of personal mobile phones to breaks and areas of the service not being used for education and care of children (ie: not in the classroom)	√	√	√	√	√
Responding to emergency phone calls only when supervising children, ensuring adequate supervision at all times *(refer to Supervision of Children Policy)*	√	√	√		√
Ensuring electronic files containing information about children and families are kept secure at all times *(refer to Privacy and Confidentiality Policy)*	√	√	√		√
Responding to a privacy breach in accordance with *Privacy and Confidentiality policy.*	√	√			
Complying with the appropriate use of social media *(refer to Definitions)* platforms *(refer to Attachment 3)*	√	√	√		√
Complying with this policy at all times to protect the privacy, confidentiality and interests of Denzil Don Kindergarten employees, children and families	√	√	√		√
BOLD tick √ indicates legislation requirement					

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 technology environment is continually changing. Early childhood services now have access to a wide variety of technologies via fixed, wireless and mobile devices. While this is a cost-effective, timely and efficient tool for 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 technology *(refer to Legislation and standards).* Illegal and inappropriate use of technology includes pornography, fraud, defamation, breach of copyright, unlawful discrimination or vilification, harassment (including sexual harassment, stalking 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. For regularly used terms e.g. Approved Provider, Nominated Supervisor, Notifiable Complaints, Serious Incidents, Duty of Care, etc. refer to the Definitions file on the Denzil Don Kindergarten website.

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

Chain email: an email that ask recipients to forward copies of an it, thus increasing circulation.

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

Cyber safety: 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: injury or harm to 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 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: encoding data before transmission so that an unauthorised party cannot decipher it.

Endpoint data storage devices: Devices capable of storing information/data. Examples include:

- laptops
- USB sticks, external or removable hard drives, thumb drives, pen drives and flash drives
- iPods or similar
- cameras with USB drive connection
- smartphones
- PCI/PC Card/PCMCIA storage cards.

Firewall: controls (by permitting or restricting) traffic into and out of a computer/network and, as a result, can protect from damage by unauthorised users.

Flash drive: data-storage device that uses flash memory and has a built-in USB connection.

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

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

Malware: short for 'malicious software', is intended to damage or disable computers or systems.

Portable storage device (PSD) *or* **removable storage device (RSD):** small, portable device capable of storing and transferring large volumes of data. These devices are either exclusively used for data storage (for example, USB key) or are capable of multiple other functions (such as iPods).

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

Social Media: technology that facilitates the sharing of ideas, thoughts, information and photos through the building of virtual networks and communities**.** Examples include but are 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.

USB key: a device that plugs into the computer's USB port. It 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 CD. Viruses can be harmful and/or dangerous: erasing data or requiring the reformatting of hard drives.

SOURCES AND RELATED POLICIES

SOURCES

- Acceptable Use Policy, DET 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
- Complaints and Grievances
- Curriculum Development
- Enrolment and Orientation
- Governance and Management of the Service
- 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

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: Laptop

AUTHORISATION

This policy was adopted by the approved provider of Denzil Don Kindergarten on 8/10/2021.

REVIEW DATE: 08 / OCTOBER / 2023

ATTACHMENT 1. PROCEDURES FOR USE OF ICT AT DENZIL DON KINDERGARTEN

Email usage

- When sending emails to multiple recipients outside of the organisation, blind copy (BCC) should always be used.
- Use an email signature that identifies name, title, service name, service phone number and includes a disclaimer *(refer to Definitions)* common to all email users to limit liability.
- Be cautious opening files or launching programs that have been received as an attachment via email.
- Check email on a regular basis and forward relevant emails to the appropriate committee/staff members.
- Respond to emails as soon as practical. Responses must be professional and include an email signature and disclaimer (see above).
- Never send unauthorised marketing content or solicitation emails.
- Never forward work emails to a personal email address – particularly those that contain sensitive information (family records, children's personal information, correspondence between Allied Health etc).

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 thus maintain privacy and confidentiality. 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)*
    - offsite storage, where there is not enough space at the service premises to store the records.

  In such circumstances, services must ensure that the information is transported, handled and stored securely so that privacy and confidentiality is maintained at all times.
- Technology users are not to view or interfere with other users' files or directories, knowingly obtain unauthorised access to information or damage, delete, insert or otherwise alter data without permission.
- Ensure all data stored on an endpoint data storage device is backed up, and that both device and backup are stored securely.

Backing up data

Denzil Don Kinder uses a cloud-based backup server.

- staff are responsible for copying their files to the cloud regularly (OneDrive or SharePoint),
- staff must not save files to their desktop without synching to the cloud regularly (at least weekly).

Password management

At Denzil Don Kindergarten, we use an online password generator to ensure passwords meet the following criteria:

- At least 8 characters in length, containing both upper and lowercase letters, at least one number and one special character (e.g. ~!@#$%^&*()_-+=).

Password users must follow the following principals:

- do not share passwords. If there is an issue that requires you to do so, change the password as soon as practical afterwards.
- never use the same password for work/personal accounts.
- do not write down passwords.
- do not store passwords electronically unless using a password manager (such as Dashlane).
- never use the "remember password" feature.
- do not use the same password for multiple administrator accounts.

Working from home

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

- complete the authorised user agreement form *(refer to Attachment 4)*

- conduct a workstation assessment; taking reasonable care to consider a suitable work space, including ergonomics, lighting, thermal comfort, safety, and privacy
- ensure security and confidentiality of work space, keeping private, sensitive, heath information, planning, educational programs and children's records confidential and secure at all times
- keep allocated passwords secure, including not sharing passwords and logging off after using a computer
- adhere to the *Privacy and Confidently Policy*
- report breaches to privacy or loss of private, sensitive, and heath information to nominated superiors as soon as practically possible.

ATTACHMENT 2. UNACCEPTABLE/INAPPROPRIATE USE OF TECHNOLOGY

Users of kinder technology (and in particular internet and email) must not:

- create or exchange messages that are offensive, harassing, obscene or threatening
- create, copy, transmit or retransmit chain emails *(refer to Definitions)*, spam *(refer to Definitions)* or other unauthorised mass communication
- use the facilities as a platform to gain unauthorised access to other systems
- forward work emails to a personal device
- carry out activities that are illegal, inappropriate or offensive to fellow employees or the public. Such activities include, but are not limited to, hate speech or material that ridicules/discriminates against others on the basis of race, nationality, creed, religion, ability/disability, gender or sexual orientation
- use the technology 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 technology 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
- conduct any outside business or engage in activities related to employment with another organisation
- play games
- use the facilities to assist any election campaign or lobby any government organisation
- exchange confidential or sensitive information held by Denzil Don Kindergarten unless authorised as part of duties
- harass, slander, intimidate, 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.

Breaches of this policy

- Individuals who use kindergarten technology 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 technology for unlawful purposes.
- The service may block access to internet sites where inappropriate use is identified.
- Employees who fail to adhere to this policy may be liable to counselling, disciplinary action or dismissal.
- Management, educators, staff, volunteers and students who fail to adhere to this policy may have their access to the service's 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
- any other material or activity that involves or is in furtherance of a breach of criminal law

Category 2: extreme — non-criminal use of material

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

This includes any material that:

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

Category 3: critical — offensive material

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

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

Category 4: serious

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

ATTACHMENT 3. SOCIAL MEDIA AND INFORMATION SHARING PLATFORM GUIDELINES

The directives below have been put in place to ensure that Denzil Don Kindergarten operates in a professional and appropriate manner when using social media and/or information sharing platforms, thus ensuring the safety and wellbeing of staff, children and their families.

Staff must exercise extreme caution when accessing social media and/or 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/guardian.

Denzil Don Kindergarten specifically requires that, unless you have the express 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(s), or otherwise share photos or videos of staff, children or families through social media;
- Do not create a Denzil Don Kindergarten branded Facebook page, or other pages or content on social media that represents Denzil Don Kindergarten, it's 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 workhours.

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 or limit staff using social media in their personal life. Staff should be aware of and understand the potential risks and damage that can be unintentionally imposed on Denzil Don Kindergarten through their use of social media, even if their activity takes place 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 which are in breach of 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 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 clearly established, the breach may be treated as grounds for dismissal. In all other cases, the person may be subject to disciplinary action in accordance with Denzil Don Kindergarten *Code of Conduct Policy*.
- Denzil Don Kindergarten may request that any information contained on any social media platform that is in breach of this policy be deleted.
- Denzil Don Kindergarten may restrict an employee's access to social media on Denzil Don Kindergarten's technology devices or if they are found to have breached this policy or while Denzil Don Kindergarten investigates whether they have breached this policy.

ATTACHMENT 4. AUTHORISED USER AGREEMENT: LAPTOP

(SENT DIGITALLY)

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 and the password that it is given to me with is not changed
    - will not be used or loaned to any person outside of Denzil Don Kindergarten
    - will be returned to Denzil Don Kindergarten on cessation of employment
    - will be stored in the case provided by the Denzil Don Kindergarten at all times.
- will immediately notify the Centre Coordinator if the laptop is damaged, faulty or lost and;
    - understand that, where damage occurs away from the kinder premises or due to a fault of my own, it is my responsibility to organise the repair of the device
- have read the Denzil Don Kindergarten Information and Communication (ICT) Technology Policy and agree to abide by the procedures outlined within.

_____ _____

Signature (authorised user) Position

_____

Date

_____ _____

Authorised by Natalie Kruger Centre Coordinator

_____

Date

Email admin@denzildonkinder.org.au