INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) POLICY

Best Practice - Quality area 7

Document classification:	Version:	Date:
Policy	**2.3**	**11/04/2024**

PURPOSE

This policy will provide guidelines to ensure that all users of information and communication technology (ICT) at Plenty Kids Early Learning Centre:

- understand and follow procedures to ensure the safe and appropriate use of ICT at the service, 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

Plenty Kids Early Learning Centre 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 ICT facilities 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.
- Provide parents/guardians with access to a copy of this document.

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 on placement and volunteers at Plenty Kids Early Learning Centre. **This policy does not apply to children.** Where services are using ICT within their educational programs, they should develop a separate policy concerning the use of ICT by children.

INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) POLICY

Best Practice - Quality area 7

This policy applies to all aspects of the use of ICT including:

- desktop top computers, laptops/notebooks, tablets, iPads, smartphones and smart devices
- copying, saving or distributing files
- electronic mail (email)
- file sharing
- file storage (including the use of end point data storage devices – *refer to Definitions*)
- file transfer/Cloud
- instant messaging
- internet usage
- portable communication devices including mobile and cordless phones.
- printing material
- social media *(refer to Definitions)*
- streaming media
- subscriptions to list servers, mailing lists or other like services
- video conferencing
- weblogs (blogs).

RESPONSIBILITIES	Approved provider and persons with management or control	Nominated supervisor and persons in day-to-day charge	Early childhood teacher, educators and all other staff	Parents/guardians	Contractors, volunteers and students
R indicates legislation requirement, and should not be deleted					
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 early childhood teachers, educators and 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 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 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. handling fees, 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 management, early childhood teachers, educators, staff and others at the service, and providing these as appropriate	√	√			
Identifying the training needs of early childhood teachers, educators and 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 information and data is limited by developing and publishing appropriate disclaimers *(refer to Definitions)*	**R**	√			
Developing procedures to ensure data and information (e.g. passwords) are kept secure, and only disclosed to individuals where necessary e.g. to new educators or staff.	**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/guardians for authorised access to the service's computer systems and internet by persons under 18 years of age (e.g. a student on placement at the service).	**R**	√			√

Providing authorisation to early childhood teachers, educators and staff to be social media representatives for Plenty Kids Early Learning Centre *(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 ICT *(refer to Attachment 2)*	√	√	√	√	√
Completing the authorised user agreement form	√	√	√		√
Maintaining the security of ICT facilities belonging to Plenty Kids Early Learning Centre 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	√	√	√		√
Obtaining approval from the approved provider before purchasing licensed computer software and hardware		√	√		
Ensuring no illegal material is transmitted at any time via any ICT medium *(refer to Attachment 2)*	**R**	√	√	√	√
Using the service's email, messaging and social media *(refer to Definitions)* facilities 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 acknowledgement form upon receipt of a portable storage device (including a laptop)		√	√		√
Ensuring electronic files containing information about children and families are kept secure at all times *(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 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 Plenty Kids Early Learning Centre employees, children and families	**R**	**R**	**R**		**R**

Procedures

Refer to *Attachment 1* for the following procedures:

- Email usage
- Digital storage of personal and health information
- Data back up
- Password management

Background and legislation

Background

The ICT environment is continually changing. Early childhood services now have access to a wide variety of technologies via fixed, wireless and mobile devices. 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 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 *General Definitions* section located on the PVCC website.

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

Chain email: An email instructing recipients to send out multiple copies of the same email so that circulation increases exponentially.

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

Cyber safety: The safe and responsible use of technology including use of the internet, electronic media and social media in order to ensure information security and personal safety. There are three main areas of risk to safety:

- Content: being exposed to illegal, inappropriate or harmful material
- Contact: being subjected to harmful online interactions with other users (including bullying)
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm.

Defamation: To injure or harm another person's reputation without good reason or justification. Defamation is often in the form of slander or libel.

Disclaimer: Statements that seeks to exclude or limit liability, usually related to issues such as copyright, accuracy and privacy.

Electronic communications: Email, instant messaging, communication through social media and any other material or communication sent electronically.

Encryption: The process of systematically encoding data before transmission so that an unauthorised party cannot decipher it. There are different levels of encryption available.

Endpoint data storage devices: Devices capable of storing information/data. New devices are continually being developed, and current devices include:

- laptops
- USB sticks, external or removable hard drives, thumb drives, pen drives and flash drives
- iPods or other similar devices
- cameras with USB drive connection
- iPhones/smartphones
- PCI/PC Card/PCMCIA storage cards
- PDAs (Personal Digital Assistants)
- other data-storage devices (CD-ROM and DVD).

Firewall: The primary method of keeping a computer/network secure. A firewall controls (by permitting or restricting) traffic into and out of a computer/network and, as a result, can protect these from damage by unauthorised users.

Flash drive: A small data-storage device that uses flash memory, and has a built-in USB connection. Flash drives have many names, including jump drives, thumb drives, pen drives and USB keychain drives.

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

Malware: Short for 'malicious software'. Malware is intended to damage or disable computers or computer systems.

PDAs (Personal Digital Assistants): A handheld computer for managing contacts, appointments and tasks. PDAs typically include a name and address database, calendar, to-do list and note taker. Wireless PDAs may also offer email and web browsing, and data can be synchronised between a PDA and a desktop computer via a USB or wireless connection.

Phishing: Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.

Portable storage device (PSD) *or* **removable storage device (RSD):** Small, lightweight, portable easy-to-use device that is capable of storing and transferring large volumes of data. These devices are either exclusively used for data storage (for example, USB keys) or are capable of multiple other functions (such as iPods and PDAs).

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

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

Social Media: A computer-based technology that facilitates the sharing of ideas, thoughts, information and photos through the building of virtual networks and communities**.** Examples can include but 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 without rebooting the computer or turning off the USB device.

USB key: Also known as sticks, drives, memory keys and flash drives, a USB key is a device that plugs into the computer's USB port and is small enough to hook onto a key ring. A USB key allows data to be easily downloaded and transported/transferred.

Virus: A program or programming code that multiplies by being copied to another program, computer or document. Viruses can be sent in attachments to an email or file, or be present on a disk or CD. While some viruses are benign or playful in intent, others can be quite harmful: erasing data or requiring the reformatting of hard drives.

Vishing: Vishing is a form of phishing that uses the phone system or voice over internet protocol (VoIP) technologies. The user may receive an email, a phone message, or even a text encouraging them to call a phone number due to some discrepancy. If they call, an automated recording prompts them to provide detailed information to verify their account such as credit card number, expiration date or birthdate.

Sources and related policies

Sources

- 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 Policy
- Compliments and Complaints Policy
- Educational Program Policy
- Enrolment and Orientation Policy
- Governance and Management of the Service Policy
- Occupational Health and Safety Policy
- Privacy and Confidentiality Policy
- Staffing Policy

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

ATTACHMENTS

- Attachment 1: Procedures for use of ICT at the service
- Attachment 2: Unacceptable/inappropriate use of ICT facilities
- Attachment 3: Social Media Guidelines
- Attachment 4: Guiding principles for security of information systems

Attachment 1

PROCEDURES FOR USE OF ICT AT THE SERVICE

Email usage

- Content of emails and email addresses must always be checked before sending.
- When sending emails to multiple recipients, care should be taken to avoid the inappropriate disclosure of email addresses to a whole group of recipients; blind copying (BCC) should be used where appropriate.
- Always include a subject description in the subject line.
- Always include a disclaimer (refer to *Definitions*) which is 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 an external storage device and scan with anti-virus software before opening, and keep an eye out for unusual filenames.
- Never open emails if unsure of the sender.
- Check email accounts on a regular basis and forward relevant emails to the Approved Provider or appropriate PVCC staff.
- Remove correspondence that is no longer required from the computer periodically.
- Respond to emails as soon as is practicable.
- Never send unauthorised marketing content or solicitation emails.
- 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 is 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)*
    - 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.
- ICT 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 material stored on an endpoint data storage device is also stored on a backup drive, and that both device and drive are kept in a secure location.

Backing up data

Data backup is the process of creating accessible data copies for use in the event of breach or loss. Plenty Kids Early Learning Centre uses both onsite and remote backup:

- Onsite Backup
  - copy data to a second hard drive, either manually or at specified intervals.
- Remote Backup- cloud based backup server
  - install the software on every computer containing data that needs to be backed up
  - set up a backup schedule
  - identify the files and folders to be copied.

Password management

The effective management of passwords is the first line of defence in the electronic security of an organisation. Plenty Kids Early Learning Centre (associated with Plenty Valley Christian College ICT facility) has a password strategy in place as part of the overall security strategy.

Technical considerations include:

- a strong password should:
  - Be at least 8 characters in length
  - Contain both upper and lowercase alphabetic characters (e.g. A-Z, a-z)
  - Have at least one numerical character (e.g. 0-9)
  - Have at least one special character (e.g. ~!@#$%^&*()_-+=)
- always verify a user's identity before resetting a password
- password rotation; changed every 90 days or less
- use of account lockouts for incorrect passwords, with a limit of 3 bad attempts.

Users should always follow these principles:

- do not share passwords with anyone. If there is an issue that requires you to do so, remember to change the password immediately after the issue has been resolved.
- never use the same password for work accounts as the one you have for personal use (banking, etc.).
- do not write down passwords or include them in an email.
- do not store passwords electronically unless they are encrypted.

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
- conduct a workstation assessment; taking reasonable care in choosing 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/INNAPROPRIATE USE OF ICT FACILITIES

Users of the ICT facilities (and in particular, the internet, email and social media) provided by Plenty Kids Early Learning Centre 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 ICT facilities as a platform to gain unauthorised access to other systems
- 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 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 Plenty Kids Early Learning Centre
- conduct any outside business or engage in activities related to employment with another organisation
- exchange any confidential or sensitive information held by Plenty Kids Early Learning Centre unless authorised as part of their duties
- publish the service's email address on a 'private' business card or digital signature
- harass, slander, intimidate, embarrass, defame, vilify, seek to offend or make threats against another person or group of people
- breach copyright laws through making copies of, or transmitting, material or commercial software.

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.
- 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 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 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 below directives are essential to the safety and wellbeing of staff, children and their families, and to ensure that Plenty Kids Early Learning Centre operates in a professional and appropriate manner when using social media and/or information sharing platforms.

Staff must exercise extreme caution using ICT facilities when accessing social media and/or information sharing platforms, whether in the workplace or relating to external events or functions involving Plenty Kids Early Learning Centre.

It is a breach of confidentiality and privacy to make posts or comments about children, families, staff or management from Plenty Kids Early Learning Centre 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.

Plenty Kids Early Learning Centre specifically requires that, unless you have the express permission, you:

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

Personal use of social media

Plenty Kids Early Learning Centre 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 Plenty Kids Early Learning Centre that can occur through their use of social media, even if their activity takes place outside working hours or on devices not owned by Plenty Kids Early Learning Centre.

If an individual can be identified as an employee of Plenty Kids Early Learning Centre 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 Plenty Kids Early Learning Centre
- expressly state on all postings (identifying them as an employee of Plenty Kids Early Learning Centre) the stated views are their own and are not those of Plenty Kids Early Learning Centre
- 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
- 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

- Plenty Kids Early Learning Centre will review any alleged breach of this policy on an individual basis. If the alleged breach is of a serious nature, the person shall be given an opportunity to be heard in relation to the alleged 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 Plenty Kids Early Learning Centre *Code of Conduct Policy*.
- Plenty Kids Early Learning Centre may request that any information contained on any social media platform that is in breach of this policy be deleted.
- Plenty Kids Early Learning Centre may restrict an employee's access to social media on Plenty Kids Early Learning Centre ICT facilities or if they are found to have breached this policy or while Plenty Kids Early Learning Centre investigates whether they have breached this policy.

Attachment 4

GUIDING PRINCIPLES FOR SECURITY OF INFORMATION SYSTEMS

The Organisation for Economic Co-operation and Development's (OECD) guidelines encourage an awareness and understanding of security issues and the need for a culture of security.

The OECD describes nine guiding principles that encourage awareness, education, information sharing and training as effective strategies in maintaining security of information systems. The guiding principles are explained in the table below.

Awareness	Users should be aware of the need for security of information systems and networks and what they can do to enhance security
Responsibility	All users are responsible for the security of information systems and networks
Response	Users should act in a timely and cooperative manner to prevent, detect and respond to security issues
Ethics	Users should respect the legitimate interest of others
Democracy	The security of information systems and networks should be compatible with the essential values of a democratic society
Risk assessment	Users should conduct risk assessments
Security design and implementation	Users should incorporate security as an essential element of information systems and networks
Security management	Users should adopt a comprehensive approach to security management
Reassessment	Users should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, measures and procedures

Sourced from Organisation for Economic Co-operation and Development's (OECD) (2002) *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security.*

DOCUMENT HISTORY AND VERSION CONTROL RECORD

Name of document: PKELC Information and Communication Technology (ICT) Policy

Responsible officer: Centre Administrator

Approved by: Principal (Approved Provider)

Assigned review period: Triennially

Date of next review: January 2027

Category: Staff & Parents

Version number	Version date	Responsible officer	Amendment details
0.1	04/12/2017	Centre Director	Initial issue as a controlled document
1.0	24/01/2019	Principal	Approved policy
2.0	02/07/2020	Centre Director	Merged original Plenty Kids Policy with ELAA Policy
2.0	19/11/2020	Centre Director	Updated Attachment 1 content
2.1	19/11/2020	Centre Director	Policy formatted in line with new style guide
2.1	19/11/2020	Principal	Approved and signed
2.2	11/04/2024	Centre Administrator	Reviewed and amended in line with ELAA recommendations
2.3	26/04/2024	Principal	Approved and signed

Approved By:

_____

John Metcalfe

26/04/2024

Date