Parkdale Preschool Association Inc A-0003637F

INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) POLICY

Best Practice – Quality Area 7

PURPOSE

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

- 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 Parkdale Preschool's *Privacy and Confidentiality Policy*
- are aware that only those persons authorised by the Approved Provider are permitted to access ICT at Parkdale Preschool
- understand what constitutes illegal and inappropriate use of ICT facilities and avoid such activities.

POLICY STATEMENT

1. VALUES

Parkdale Preschool is committed to:

- professional, ethical and responsible use of ICT at Parkdale Preschool
- providing a safe workplace for management, educators, staff and others using the service's ICT facilities
- safeguarding the privacy and confidentiality of information received, transmitted or stored electronically
- ensuring that the use of Parkdale Preschool'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 Parkdale Preschool.

2. SCOPE

This policy applies to the Approved Provider, Nominated Supervisor, Educators, staff, students on placement and volunteers at Parkdale Preschool. This policy does **not** apply to children.

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

- internet usage
- electronic mail (email)
- electronic bulletins/notice boards
- electronic discussion/news groups
- blogs
- social networking
- file transfer
- file storage (including the use of end point data storage devices – refer to *Definitions*)
- file sharing
- video conferencing
- streaming media
- instant messaging

- social media
- online discussion groups and chat facilities
- subscriptions to list servers, mailing lists or other like services
- copying, saving or distributing files
- viewing material electronically
- printing material
- portable communication devices including iPads, mobile and cordless phones.

3. BACKGROUND AND LEGISLATION

Background

The Victorian Government has funded the provision of ICT infrastructure and support to kindergartens since 2003. This support has included:

- purchase and installation of ICT equipment
- installation and maintenance of internet connection
- provision of email addresses
- training in the use of software and the internet
- help desk support.

The purpose of this support is to:

- establish ICT infrastructure to assist teachers in the development and exchange of learning materials, and in recording children's learning
- contribute to the professional development of kindergarten teachers and assistants, and enhance their access to research in relation to child development
- establish ICT infrastructure that enhances the management of kindergartens and reduces the workload on management committees
- contribute to the sustainability of kindergartens by providing for the better management of records, including budget and finance records (IT for Kindergartens: www.kindergarten.vic.gov.au).

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* (Vic), as amended 2007
- *Charter of Human Rights and Responsibilities Act 2006* (Vic), as amended 2011
- *Classification (Publications, Films and Computer Games) Act 1995*
- *Commonwealth Classification (Publication, Films and Computer Games) Act 1995*, as amended 2007
- *Competition and Consumer Act 2010* (Cth)
- *Copyright Act 1968* (Cth)
- *Copyright Amendment Act 2006* (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*
- *Privacy Act 1988* (Cth)
- *Public Records Act 1973* (Vic)
- *Sex Discrimination Act 1984* (Cth)
- *Spam Act 2003*
- *Trade Marks Act 1995* (Cth)

4. DEFINITIONS

The terms defined in this section relate specifically to this policy.

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.

C**loud drive:** A Web-based service that provides storage space on a remote server.

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.

Confidentiality: The privacy of personal or corporate information. This included issues of copyright. Confidentiality of information is mandated by common law, formal statute, explicit agreement or convention. Different classes of information warrant different degrees of confidentiality.

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

Disclaimer: Statement(s) that seeks to exclude or limit liability and is usually related to issues such as copyright, accuracy and privacy. A disclaimer will usually include:

- A warning to all recipients that the contents of the email may contain personal information and that privacy should be respected at all times
- A statement that the email is intended to the addressee only and, if anyone else receives it the steps that person should take, such as "inform the sender that personal information has been misdirected and delete the personal information".

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

- iPads, 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.

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).

Spam: Unsolicited and unwanted emails or other electronic communication.

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

USB 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.

Vicnet: An organisation that provides a range of internet services to libraries and community groups (including kindergartens, as part of a government-funded project), including broadband and dial-up internet and email access, website and domain hosting, and website design and development. Vicnet delivers information and communication technologies, and support services to strengthen Victorian communities. For more information, visit www.kindergarten.vic.gov.au

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.

5. SOURCES AND RELATED PARKDALE PRESCHOOL POLICIES

Sources

- *Acceptance Use Policy*, DET Information, Communications and Technology (ICT) Resources: https://www.education.vic.gov.au/school/principals/spag/infrastructure/pages/ictsecurity.aspx
- IT for Kindergartens: www.kindergarten.vic.gov.au
- Organisation for Economic Co-operation and Development (OECD) (2002) *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* www.oecd.org

Parkdale Preschool policies

- *Staff Code of Conduct Policy*
- *Complaints and Grievances Policy*
- *Enrolment and Orientation Policy*
- *Governance and Management of the Service Policy*
- *Occupational Health and Safety Policy*
- *Privacy and Confidentiality Policy*
- *Staffing Policy (Includes Determining Responsible Person)*

PROCEDURES

The Approved Provider is responsible for:

- ensuring that the use of Parkdale Preschool'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 *Staff Code of Conduct Policy*)
- providing suitable ICT facilities to enable educators and staff to effectively manage and operate the service
- providing clear procedures and protocols that outline the parameters for use of Parkdale Preschool's ICT facilities (refer to Attachment 1 – Procedures for use of ICT at Parkdale Preschool)
- embedding a culture of awareness and understanding of security issues at Parkdale Preschool (refer to Attachment 1 – Guiding principles for security of information systems)
- ensuring that effective financial procedures and security measures are implemented where transactions are made using Parkdale Preschool's ICT facilities, e.g. handling fee and invoice payments, and using online banking
- ensuring that Parkdale Preschool's ICT software and hardware are purchased from appropriate and reputable suppliers
- identifying the need for additional password-protected email accounts for management, educators, staff and others at Parkdale Preschool, and providing these as appropriate
- identifying the training needs of educators and staff in relation to ICT, and providing recommendations for the inclusion of training in ICT in professional development activities
- ensuring that procedures are in place for the regular backup of critical data and information
- ensuring secure storage of all information at and belonging to Parkdale Preschool, 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 Parkdale Preschool's computer/s, including emails and cloud drives
- considering encryption (refer to *Definitions*) of data for extra security
- ensuring that reputable anti-virus and firewall software (refer to *Definitions*) are installed on Parkdale Preschool 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*)
- ensuring that Parkdale Preschool'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 passwords are changed regularly, kept secure, and only disclosed to individuals where necessary e.g. to new educators, staff or committee of management
- developing procedures to ensure that all educators, staff, volunteers and students are aware of the requirements of this policy
- ensuring the appropriate use and backup of endpoint data storage devices (refer to *Definitions*) by all ICT users at Parkdale Preschool
- ensuring compliance with this policy by all users of Parkdale Preschool's ICT facilities ensuring that written permission is provided by parents/guardians for authorised access to Parkdale Preschool's computer systems and internet by persons under 18 years of age (e.g. a student on placement at Parkdale Preschool) (refer to Parkdale Preschool Volunteers and Students Induction Checklist).

The Nominated Supervisor, Educators, staff and other authorised users of Parkdale Preschool's ICT facilities are responsible for:

- complying with all relevant legislation and Parkdale Preschool policies, protocols and procedures, including those outlined in the policy Attachment
- keeping allocated passwords secure, including not sharing passwords and logging off after using a computer
- users of personal devices should ensure that they have password protection on that device, and that any files downloaded onto the personal device are deleted once they've been saved back onto the shared drive.
- maintaining the security of ICT facilities belonging to Parkdale Preschool
- accessing accounts, data or files on Parkdale Preschool's computers and cloud drives only where authorisation has been provided
- cooperating with other users of Parkdale Preschool's ICT to ensure fair and equitable access to resources
- obtaining approval from the Approved Provider before purchasing licensed computer software and hardware
- ensuring confidential information is transmitted with password protection or encryption, as required
- ensuring no illegal material is transmitted at any time via any ICT medium
- using Parkdale Preschool's email, messaging and social media facilities for service-related and lawful activities only
- using endpoint data storage devices and cloud drives (refer to *Definitions*) supplied by Parkdale Preschool 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 ICT equipment
- restricting the use of personal mobile phones and messaging devices (such as smartwatches) to rostered breaks
- responding only to emergency phone calls when responsible for supervising children to ensure adequate supervision of children at all times (refer to *Interactions with children Policy*)
- ensuring electronic files containing information about children and families are kept secure at all times (refer to *Privacy and Confidentiality Policy*).
- We strongly advise staff not to accept friend requests from current families. Staff are recommended to have their social media accounts set to the highest privacy settings.

Parents/guardians are responsible for:

- reading and understanding this *Information and Communication Technology (ICT) Policy*
- complying with all state and federal laws, the requirements of the *Education and Care Services National Regulations 2011*, and all Parkdale Preschool policies and procedures
- maintaining the privacy of any personal or health information provided to them about other individuals e.g. contact details.

Volunteers and students, while at Parkdale Preschool, are responsible for following this policy and its procedures.

Guidelines for safe use of social media in your early childhood service

1. Social media refers to sites such platforms as Facebook, Twitter, YouTube or Instagram (and others) where information can be published to a public audience and members of the network can react or publish information also.
2. Social Media Channels can be used as a tool for easily communicating about the Preschool; therefore it should at all times be viewed and used as an extension of our business communication systems
3. The Committee of Management **with the approval of Educational Leader/Administration** will be responsible for identifying and maintaining its official social media profiles, and this policy relates primarily to the content published on these official profiles.
4. The objective of official social profiles is to share information about our service and make information about the preschool discoverable. This may include updates like:
    a. Photographs about the learning environment and learning experiences
    b. Articles of interest
    c. Updates specific to our service or the early childhood sector
    d. Announcements about social events, fundraising projects, and other preschool community information.
5. it is important to pay careful attention to how and what we share over the internet in order to ensure we respect and protect the privacy of children, staff, families and anyone associated with our service at all times. This may mean that face-shots should not be published without written consent of that adult person, or their parent in the case of a child.
6. Social networks also offer paid advertising opportunities which may be used for promotional purposes, subject to budget approval.
7. The committee should allocate a member of staff or committee representative to monitor the official social media profiles, inappropriate comments and make sure uploading of video and photos respect our Privacy and Confidentiality Policy.
8. The privacy of staff should be respected and their personal profiles should not be tagged when the official social media channel is posting information or updates.
9. A separation of professional and personal life should be respected and therefore staff and employees are encouraged not to accept connection/friend requests from parents or colleagues.

Due to the changing nature of social media platforms and options, this policy may be expanded into more specific policies in time. The Committee Of Management may decide supplement this policy with more specific tactics and best practices that it needs to guide its goals for the current year.

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 Parkdale Preschool's policy review cycle, or as required
- notify parents/guardians at least 14 days before making any changes to this policy or its procedures.

ATTACHMENTS

- Attachment 1: Procedures for use of ICT at Parkdale Preschool

AUTHORISATION

This policy was adopted by the Approved Provider of Parkdale Preschool on 19th March 2020

REVIEW DATE: MARCH 2023