




**Parkdale Preschool Association
Policy Document**

	<p align="center">Parkdale Preschool Association Policy Document</p>
Policy No. AO1-12-00	Title: Information technology
	Function: Administration and Operation
	Review Cycle: 24 months

Document/Revision History

Policy Revision #	Issue Date	Description of Changes	Superseded Document #

Purpose

This policy will provide guidelines to ensure that all users of information technology facilities at **Parkdale Preschool** or on behalf of **Parkdale Preschool** are aware of:

- Their responsibilities to protect and maintain privacy in accordance with the centre's Privacy policy
- The procedures to follow to ensure safe and appropriate use of the centre's information technology facilities
- Who has authorised access to the various components of the centre's information technology facilities
- The OECD's nine guiding principles for users of information technology facilities. (see [Attachment 2](#): Guiding principles for security of information systems)

Policy statement

Values

Parkdale Preschool is committed to:

- The professional, ethical and responsible use of information technology facilities at the **Parkdale Preschool**
- Providing a safe workplace for employees, the employer and others using the centre's information technology facilities
- Maximising the protection needed to safeguard the privacy and confidentiality of information received, transmitted or stored electronically
- Ensuring the use of the centre's information technology facilities complies with the centre's policies and relevant legislation
- Providing its employees and committee with online information resources and communication tools to support the effective operation of the centre.

Scope

This policy applies to employees, committees, students on placement, volunteers and any other persons who have access to or use information technology facilities at **Parkdale Preschool**.

This policy governs access to the Internet, electronic mail (email), portable memory sticks (USB) and other information technology facilities within the centre. Use of portable communication devices, such as mobile and cordless phones, is also covered by this policy.

Background and legislation

The information technology (IT) environment is continually changing. Centres now have access to a variety of technology options via fixed, wireless and mobile devices. The Internet is a wonderful resource for research and communication and for conducting business. However, this new environment has raised new issues for centres to consider in regard to information privacy, security and sharing.

The Victorian Government funds the provision of IT infrastructure and ongoing support that:

- Assists teachers in the development and exchange of learning materials

-
- Contributes to the professional development of kindergarten teachers and assistants, and enhances their access to research in relation to child development
 - Establishes an IT infrastructure that enhances the management of kindergartens and reduces the workload on management committees
 - Contributes to the sustainability of kindergartens by providing for the better recording of records, including budgets and finance plans.

Relevant legislation may include but is not limited to:

- *Children's Services Act 1996*
- Children's Services Regulations 2009
- *Health Records Act 2001 (Vic.)*
- *Information Privacy Act 2000 (Vic.)*
- *Privacy Act 2000*
- Censorship legislation
- *Spam Act 2003 (Cwlth)*
- *The Occupational Health & Safety Act 2004*
- *Trade Marks Act 1955 (Cwlth)*
- *Trade Practices Act 1974 (Cwlth)*
- *Copyright Act 1968 (Cwlth).*

Definitions

Anti-spyware: Software that removes small files that have been placed on your computer as you browse the Internet. Spyware allows Internet users to record what websites you have visited and sell this information to marketing companies.

Chain mail: Email sent to a number of people asking the recipient to send copies of the email with the same request to a number of recipients

Computer virus: Allows Internet users to make your computer do things without your permission. Common viruses can send emails to everyone in your address book, change browser settings or steal files from your computer.

Confidentiality: The privacy of personal or corporate information. This includes 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: Injure or harm another's reputation without good reason or justification; slander or libel.

Department of Education and Early Childhood Development (DEECD): The state government department responsible for the funding, licensing and regulation of children's services in Victoria.

Disclaimer: Statement that seeks to exclude or limit liability and usually deals with 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 for 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'.

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

End point data-storage devices: A device capable of having information/data copied on to them. New devices are continually emerging and include:

- USB sticks, drives, thumb nails, pen drives, flash drives
- iPods
- Cameras with USB drive connection
- iPhones/Smartphones
- PCI/PC Card/PCMCIA storage cards
- PDAs
- Other data-storage devices (CD-ROM, DVD).

Firewall: Blocks viruses and other malicious software from running on your machine. It works by limiting the number and type of connections available to the Internet.

Flash drive: Flash drives have many names—jump drives, thumb drives, pen drives and USB keychain drives. Regardless of what you call them, they all refer to the same thing, which is a small data-storage device that uses flash memory and has a built-in USB connection.

Information technology (IT) facilities: Includes communication devices, such as mobile/cordless phones, computers, networks, Internet access, email, hardware, dial-up access, end point data-storage devices, computer accounts and software.

Integrity: In relation to this policy, refers to the accuracy of data. Loss of data integrity may be either gross and evident (such as when a computer disk fails) or subtle (such as when a character in a file is altered).

Portable storage device (PSD)/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.

Security: Can be defined as 'the state of being free from unacceptable risk'. The risk concerns the following categories of losses: confidentiality of Information; integrity of data assets; efficient, appropriate use and system availability.

USB interface: Universal Serial Bus 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 device.

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

Vicnet: Provides a range of Internet services to community groups (including kindergartens as part of a government-funded project) and libraries, including broadband and dial-up Internet and email access, website and domain hosting, and website design and development. It delivers information and communication technologies and support services that aim to strengthen Victorian communities.

Virus: A program or programming code that replicates 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 causing your hard disk to require reformatting.

Sources and related centre policies

Sources

- Organisation for Economic Cooperation and Development (OECD) 2002, Guidelines for the *Security of Information Systems and Networks: Towards a Culture of Security*

Centre policies

- Code of conduct
- Communication
- Occupational health and safety
- Privacy
- Program participation

Procedures

The committee is responsible for:

- Providing suitable IT facilities to enable staff, committee and volunteers to effectively manage and operate the centre
- Authorising members of staff, committee, volunteers and student's access to the centre's IT facilities.
- Providing clear procedures and protocols outlining the parameters for usage of the centre's IT facilities (see [Attachment 1](#), 'Procedures for use of emails and IT facilities')
- Ensuring effective financial procedures are in place if transactions are made using the centre's IT facilities, such as fee and invoice payments and online banking
- Ensuring programs loaded on to the centre's computer are purchased from an appropriate supplier
- Identifying the need for additional password-protected email accounts for staff, committee members and any other persons requiring access to email facilities at the centre
- Identifying training needs of staff and providing recommendations for inclusion in professional development
- Ensuring procedures are in place for the regular backup of critical data and information
- Ensuring secure storage of all backup information
- Reviewing centre policies, practices, measures and procedures to ensure that the centre meets the evolving challenges posed by threats to information systems and networks (virus protection)
- Adhering to the Privacy policy requirements in regard to all emails and information accessed on the centre's computer
- Completing a risk assessment to determine the level of encryption, if any, that is required
- Ensuring reputable anti-virus and firewall software are installed and kept up to date

-
- Developing procedures to minimise exposure to unauthorised access, use and disclosure through limiting access, passwords, use of disclaimers and encryption
 - Developing procedures that ensure information such as passwords are kept securely but known to more than one person, including passing on to new staff/committee members
 - Developing procedures to ensure all staff, volunteers and students are aware of the requirements of this policy
 - Appropriate use of end point data-storage devices is permitted for business purposes and justification will be sought for files copied to and from end point data-storage devices, of any description, including the storage of data on devices that can be connected either by USB, data cable or wireless connection direct to any computer equipment within the organisation
 - Ensuring compliance with this policy by all users of the centre's IT facilities
 - Ensuring students on placement have provided written permission by their parents/guardians (see [Attachment 3](#), 'Parent/Guardian authorisation for under-age access to the **Parkdale Preschool** IT facilities) if they under 18 years, before being given authorised access to the centre's computers (namely the Internet).

The committee is not responsible for:

- Loss or damage, or consequential loss or damage, arising from the use of the centre's IT facilities (for example, banking transactions or purchases made via the internet).

Each authorised user is responsible for:

- Compliance with relevant legislation and centre policies, protocols and procedures, including those outlined in [Attachments 1](#) and [2](#)
- Completing the Authorised user agreement form (see [Attachment 4](#))
- Keeping the password allocated to them by the committee secure, including not sharing passwords and logging off after using a computer
- Not compromising or attempting to compromise the security of any IT facility belonging to "[insert centre name]", nor exploit or attempt to exploit any security deficiency
- Using the IT facilities in an ethical and lawful way in accordance with Australian laws (refer to legislation listed in this document)
- Only accessing accounts, data or files on the centre's computers that they have authorisation to access
- Cooperating with other users of the IT facilities to ensure fair and equitable access to the facilities
- Obtaining committee approval before purchasing licensed software and hardware for installation on the centre computer/s
- Not transmitting confidential information unless it is encrypted
- Not attempting to access or transmit at any time via email or any other medium material that is illegal
- Being aware of the need for the security of information systems and the network and what they can do to enhance security, including acting in a timely and cooperative manner to prevent, detect and respond to security incidents and report any concerns to the committee
- Only using the centre's email and messaging facilities for centre-related activities, provided such use is lawful. Messaging facilities may include chat sessions (for example, with other professionals) and electronic conferences (where applicable). The

committee reserve the right to withdraw this permission in the event that such use places the IT facilities at risk or poses a security or other threat

- Only using the end point data-storage device for its intended business purpose and ensuring that information contained or transmitted via these resources is protected from unauthorised use, copying or modification
- Not using end point data-storage devices as the primary storage medium for **Parkdale Preschool** documents
- Recognising that end point data-storage devices are provided as work tools and belong to the **Parkdale Preschool**
- Notifying the committee of any faults with end point data-storage devices
- Notifying the committee of the loss of any end point data-storage devices
- Signing acknowledgement forms on receipt of USBs. (See [Attachment 4](#): Authorised user agreement)

Staff working with children are responsible for:

- Restricting the use of personal mobile phones to rostered breaks
- Responding to emergency phone calls only when they are responsible for supervising children and keeping those calls as brief as possible; other callers should be requested to call back during the staff members non-contact time
- Maintaining supervision of the children at all times.

Evaluation

In order to assess whether this policy has achieved its values and purposes, the committee will:

- Monitor complaints received in relation to the use of the centre's computer and online resources
- Review compliance and any breaches of this policy to determine if alterations are required
- Take into account reports from employees, committee, parents/guardians and any other persons in relation to the policy
- Keep up-to-date with current research and new technology.

Attachments

[Attachment 1](#): Procedures for use of emails and IT facilities

[Attachment 2](#): Guiding principles for security of information systems

[Attachment 3](#): Parent/Guardian authorisation for under-age access to the **Parkdale Preschool** IT facilities

[Attachment 4](#): Authorised user agreement

Authorisation

This policy was adopted by the **Parkdale Preschool** committee of management at a committee meeting on.

Review date: 17 /NOV /2010

Procedures for use of emails and IT facilities

- Content of emails and addresses must always be checked before sending.
- When sending to multiple recipients, care should be taken to avoid the disclosure of other email details; use of BCC where appropriate.
- Always include the subject in the subject line.
- Include a disclaimer on all emails, which will provide some security to the **Parkdale Preschool**.
- Never open files or start programs that have been sent as an attachment via email; instead, save an attachment to disk and scan with anti-virus software before you open it and check for unusual filenames.
- Never open emails if you are unsure of the sender.
- Check email accounts on a regular basis (for example, bi-weekly) and forward relevant emails to appropriate members of the committee and staff.
- Remove outdated and unused emails from the computer quarterly.
- Respond to emails as soon as practicable.
- Consider the risks and determine whether or not to send personal and sensitive information via unencrypted email.
- Ensure all material stored on an end point data-storage device is also stored on a backup drive.

Unacceptable use of IT facilities

Users of the Internet and email access provided by **Parkdale Preschool** may not use these facilities to:

- Create or exchange messages that are offensive, harassing, obscene or threatening
- Create, copy, transmit or retransmit chain letters, spamming or other unauthorised mass mailings
- Use **Parkdale Preschool** IT 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 others on the basis of race, creed, religion, colour, sex, disability, national origin or sexual orientation
- Visit websites containing objectionable (including pornographic) or illegal material
- Make any personal communication that could create the perception that the communication was made in that person's official capacity as an employee or volunteer of **Parkdale Preschool**
- Conduct any outside business or private employment
- Play games
- Assist any election campaign or lobby any government organisation
- Exchange any confidential or sensitive information held by **Parkdale Preschool** unless authorised as part of their duties

-
- Not utilising the centre's IT facilities to access pornographic material or to create, store or distribute pornographic material—it will not be a defence to claim that the recipient was a consenting adult
 - Not publishing the centre email address on a 'private' business card
 - Ensuring email or any other medium is not used to harass, slander, intimidate, embarrass, defame, vilify, and seek to offend or make threats against another person or group of people
 - Ensuring email or any other medium is not used to access or transmit at any time material (language and images) that a reasonable person could consider indecent, offensive, obscene, profane, sexually explicit or objectionable
 - Ensuring copyright is not breached through making copies of, or transmitting material, or commercial software.

Information stored on computers

- Records containing personal, sensitive, health information or photographs of children will be stored securely so that the privacy and confidentiality of all information are maintained. For example, password protected or transferred to remote storage device—that is, CD-ROM and memory stick—and kept in a secure location.
- Users of the computers are not to view or interfere with other users' files or directories (for example, staff/committee) or knowingly obtain unauthorised access to information or damage, delete, insert or otherwise alter data without permission.

Breaches of this policy

- Users who fail to adhere to the procedures set out in this policy may be liable to personal 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 even imprisonment. The committee will not defend or support any user who uses the IT facilities for an unlawful purpose.
- The centre may have access to Internet sites blocked where inappropriate use is identified.
- Employees failing to adhere to this policy may be liable to counselling or disciplinary action.
- Committee members, volunteers and students failing to adhere to the policy may have access to the centre's computers denied.

Guiding principles for security of information systems

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

The OECD provides nine guiding principles that are supported through awareness, education, information sharing and training. These 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.

The Organisation for Economic Cooperation and Development's (OECD) 2002, *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*

Parent/Guardian authorisation for under-age access to the Parkdale Preschool IT facilities

Student's name: _____

Date of placement: _____

I, _____, am a parent or legal guardian of
_____.

I have read the **Parkdale Preschool** Information technology policy and agree to the conditions of use for the IT facilities for the above-named student.

I also understand that **Parkdale Preschool** provides no censorship for anything a student may access.

Signed: _____ Date: _____

(Student)

Signed: _____ Date: _____

(Parent/Guardian)

Authorised user agreement

I, _____,

- Acknowledge that I have received a Personal Storage Device belonging to **Parkdale Preschool**
- Will ensure that the PSD is:
 - Used for work-related purposes only
 - Is password protected at all times
 - Will not be loaned to anyone outside the organisation
 - Will be returned to **Parkdale Preschool** on cessation of employment
- Will notify the **Director** as soon as practicable if the PSD is lost or misplaced at any time
- Have read the **Parkdale Preschool** Information technology policy and agree to abide by the guidelines included in this policy.

Signed: _____

Position: _____

Date: _____

Authorised by: _____

Position: _____

Date: _____