SOMERVILLE KINDERGARTEN INCORPORATED

Information and Communication Technology

Best Practice – Quality Area 7

PURPOSE

This policy will provide guidelines to ensure that all users of information and communication technology (ICT) at Somerville Kindergarten or on behalf of Somerville Kindergarten. 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. Be 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.

VALUES

Somerville Kindergarten is committed to the 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. Safeguarding the privacy and confidentiality of information received, transmitted or stored electronically. Ensuring that the use of the service 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.

SCOPE

This policy applies to the Approved Provider, Persons with Management and Control, Nominated Supervisor, Persons in Day to Day Charge, educators, staff, students on placement and volunteers at Somerville Kindergarten. 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.

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
- weblogs (blogs)
- social networking
- file transfer
- file storage (including the use of end point data storage devices
- file sharing
- video conferencing
- streaming media
- instant messaging
- 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 mobile and cordless phones.

IMPLEMENTATION

The child may only leave the service in the care of a parent/guardian, authorised nominee, or a person authorised by one of these parties to collect the child. An authorised person does not include a parent who is prohibited by court order from having contact with the child.

Management / Approved Provider will be responsible for:

- ensuring that the use of the service's ICT complies with all relevant state and federal legislation and all service policies (including *Privacy and Confidentiality Policy* and *Code of Conduct Policy*)
- providing suitable ICT facilities to enable educators and staff to effectively manage and operate the service
- authorising the access of 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
- 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 service's ICT facilities, e.g. handling fee and invoice payments, and using online banking
- 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, educators, staff and others at the service, 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 at the service
- ensuring secure storage of all information at the service, including backup files
- adhering to the requirements of the *Privacy and Confidentiality Policy* in relation to accessing information on the service's computer/s, including emails
- considering encryption of data for extra security
- ensuring that reputable anti-virus and firewall software 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
- 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
- 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, 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 of endpoint data storage devices by all ICT users at the service
- 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
- ensuring compliance with this policy by all users of the service's ICT facilities
- 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)

Nominated supervisor / Responsible person & Educators will:

- comply with all relevant legislation and service policies, protocols and procedures, including those outlined in Attachments 1 and 2
- complete the authorised user agreement form
- keep allocated passwords secure, including not sharing passwords and logging off after using a computer
- maintain the security of ICT facilities belonging to Somerville Kindergarten
- access accounts, data or files on the service's computers only where authorisation has been provided
- co-operate with other users of the service's ICT to ensure fair and equitable access to resources
- obtain approval from the Approved Provider before purchasing licensed computer software and hardware
- ensure confidential information is transmitted with password protection or encryption, as required
- ensure no illegal material is transmitted at any time via any ICT medium

- use the service's email, messaging and social media facilities for service-related and lawful activities only
- use endpoint data storage devices supplied by the service for service-related business only, and ensure that this information is protected from unauthorised access and use
- ensure that 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
- notify the Approved Provider of any damage, faults or loss of endpoint data storage devices
- sign an acknowledgement form upon receipt of a USB or portable storage device (including a laptop)
- restrict the use of personal mobile phones to rostered breaks
- respond only to emergency phone calls when responsible for supervising children to ensure adequate supervision of children at all times
- ensure electronic files containing information about children and families are kept secure at all times
- respond to a privacy breach in accordance with privacy and confidentiality policy.

Families will:

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

All Volunteers and students, whilst at Somerville Kindergarten, are responsible for following this policy and its procedures. Staff to always make sure that they are aware of all policies and procedures before commencing.

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 (refer to Kindergarten IT Program: http://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:

- 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)
- 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)
- 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: http://www.legislation.vic.gov.au
- Commonwealth Legislation – ComLaw: http://www.comlaw.gov.au/

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 parents/guardians at least 14 days before making any changes to this policy or its procedures.

DEFINITIONS

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.

Spam: Unsolicited and unwanted emails or other electronic communication.

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.

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

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:

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.

SOURCES

Relevant legislation and standards include but are not limited to:

- *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 Policy
- Complaints and Grievances Policy

- Curriculum Development Policy
- Enrolment and Orientation Policy
- Governance and Management of the Service Policy
- Occupational Health and Safety Policy
- Privacy and Confidentiality Policy
- Staffing Policy

ATTACHMENTS

- Attachment 1: Procedures for use of ICT at the service
- Attachment 2: Guiding principles for security of information systems
- Attachment 3: Parent/guardian authorisation for under-age access to the ICT facilities
- Attachment 4: Authorised user agreement

ATTACHMENT 1: PROCEDURES FOR THE 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 disk 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 committee members/staff.
- Remove correspondence that is no longer required from the computer quarterly.
- Respond to emails as soon as is practicable.

Unacceptable/inappropriate use of ICT facilities:

Users of the ICT facilities (and in particular, the internet, email and social media) provided by Somerville Kindergarten must not:

- create or exchange messages that are offensive, harassing, obscene or threatening
- create, copy, transmit or retransmit chain emails spam 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 Somerville Kindergarten
- conduct any outside business or engage in activities related to employment with another organisation
- play games
- assist any election campaign or lobby any government organisation
- exchange any confidential or sensitive information held by Somerville Kindergarten unlesss authorised as part of their duties
- publish the service's email address on a 'private' business card
- 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.

Information stored on computers:

- Computer records containing personal, sensitive and/or health information, or photographs of children must be 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*).
- Computer 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
- 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.
- Computer 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.

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.

ATTACHMENT 2: 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.*

ATTACHMENT 3: PARENT/GUARDIAN AUTHORISATION FOR UNDER-AGE ACCESS TO THE SOMERVILLE KINDERGARTEN ICT FACILITIES

Student Name: _____

Placement date: _____

I, _____, am a parent/guardian of

_____

I have read the Somerville Kindergarten Information and Communication Technology (ICT) Policy and agree to the conditions of use of the Service's ICT facilities for the above-named student.

I also understand that Somerville Kindergarten provides no censorship of access to ICT facilities.

_____ ____/____/_____
Signature (Student) Date

_____ ____/____/_____
Signature (parent/guardian) Date

ATTACHMENT 4: AUTHORISED USER AGREEMENT

Portable storage device (PSD) (Including laptops)

I, _____
acknowledge that I have received a PSD belonging to Somerville Kindergarten.

I will ensure that the PSD:

- Is used for work-related purposes only
- Is password-protected at all times
- Will not be loaned to unauthorised persons
- Wil be returned to Somerville Kindergarten on cessation of employment

I will notify the President as soon as practicable if the PSD is damaged, faulty or lost.
I have read the Somerville Kindergarten Information and Communication Technology Policy and agree to abide by the procedures outlines within.

_____ _____
Signature (authorised user) Position

____/____/_____
Date

_____ _____
Authorised by Position

____/____/_____
Date