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 Eureka Community Kindergarten Association Inc. (ECKA) or on behalf of Eureka Community Kindergarten Association Inc. (ECKA):

- understand and follow procedures to ensure the safe and appropriate use of ICT at the service, including maintaining secure storage of information / data and technology infrastructure
- 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 the security measures that have been developed to help mitigate security risks

POLICY STATEMENT

1. VALUES

Eureka Community Kindergarten Association Inc. (ECKA) 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
- 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.

2. SCOPE

This policy applies to the Approved Provider, Nominated Supervisor, Certified Supervisor, educators, staff, students on placement and volunteers at Eureka Community Kindergarten Association Inc. (ECKA). This policy does **not** apply to children.

This policy applies to all aspects of the use of ICT including, but not limited to:

- 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 – refer to *Definitions*)
- 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.

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 (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:

- *Broadcasting Services Act 1992 (Cth)*
- *Charter of Human Rights and Responsibilities Act 2006* (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 2017* (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)
- *Privacy and Data Protection Act 2014 (Vic)*
- *National Quality Standard*, Quality Area 7: Leadership and Service Management
  - Standard 7.3: Administrative systems enable the effective management of a quality service
- *Occupational Health and Safety Act 2004* (Vic)
- *Privacy Act 1988* (Cth)
- *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/

4. DEFINITIONS

The terms defined in this section relate specifically to this policy. For commonly used terms e.g. Approved Provider, Nominated Supervisor, Regulatory Authority etc. refer to the *General Definitions* section of this manual.

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, and that may harm a computer system's data or performance.

Cyber Security: Cyber security refers to measures relating to the confidentiality, availability and integrity of information and data that is processed, stored and communicated by electronic or similar means, protecting it and associated systems from external or internal threat.

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.

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.

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 POLICIES

Sources

- *Acceptance Use Policy*, DET Information, Communications and Technology (ICT) Resources: www.education.vic.gov.au/about/deptpolicies/acceptableuse.htm
- 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

Service 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*

PROCEDURES

The Approved Provider is responsible for:

- 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*)
- 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 (refer to Attachment 1 – Procedures for use of ICT at the service)
- embedding a culture of awareness and understanding of security issues at the service (refer to Attachment 2 – Guiding principles for security of information systems)
- 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 (refer to *Privacy and Confidentiality Policy*)
- adhering to the requirements of the *Privacy and Confidentiality Policy* in relation to accessing information on the service's computer/s, including emails
- ensuring 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*)

- ensuring that the service's liability in the event of security breaches, or unauthorised access, use and disclosure of information and data is limited by developing and publishing appropriate disclaimers (refer to *Definitions*)
- developing procedures to ensure data and information (e.g. passwords) are kept secure, and only disclosed to individuals where necessary e.g. to new educators or staff
- 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 (refer to *Definitions*) 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) (refer to Attachment 4 – Parent/guardian authorisation for under-age access to the Eureka Community Kindergarten Association Inc. (ECKA) ICT facilities).
- Arrange for security training for all employees.
- Inform employees regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.
- Follow this policies provisions as other employees do.

The Nominated Supervisor, Certified Supervisors, educators, staff and other authorised users of the service's ICT facilities are responsible for:

- complying with all relevant legislation and service policies, protocols and procedures, including those outlined in Attachments 1 and 2
- keeping allocated passwords secure, including not sharing passwords and logging off after using a computer
- maintaining the security of ICT facilities belonging to Eureka Community Kindergarten Association Inc. (ECKA)
- 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 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 the service's email, messaging and social media facilities for service-related and lawful activities only
- 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
- ensuring 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
- notifying the Approved Provider of any damage, faults or loss of endpoint data storage devices
- restricting the use of personal mobile phones 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 *Supervision of Children Policy*)
- ensuring electronic files containing information about children and families are kept secure at all times (refer to *Privacy and Confidentiality Policy*).

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 service 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 the service, are responsible for following this policy and its procedures.

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

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 Eureka Community Kindergarten Association Inc. (ECKA) ICT facilities

AUTHORISATION

This policy was adopted by the Eureka Community Kindergarten Association Inc. (ECKA) on 16/10/15.

Operational Procedures may be modified as per the delegations policy to meet ECKA's needs.

Last Reviewed: 19/06/18

REVIEW DATE: 1/06/20

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 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 staff member.
- 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 Eureka Community Kindergarten Association Inc. (ECKA) 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 Eureka Community Kindergarten Association Inc. (ECKA)
- 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 Eureka Community Kindergarten Association Inc. (ECKA) unless 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.
- access internal systems and accounts from another's device or lend their own device to others.

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. When taken off-site, confidential information can only be accessed by authorised personnel with a password. (refer to *Privacy and Confidentiality Policy*).
- 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 a hard drive (desktop/ lap top /iPad/ tablet or any other electronic device) is also stored on a backup drive (usb or external hard drive) and that both device and drive are kept in a secure location.

MANAGE PASSWORDS

Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they won't be easily hacked, but they should also remain secret. For this reason, we advise our employees to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays.)
- Services need to incorporate risk management measures to ensure that passwords are recorded and stored in a secure place at the service and to limit access to the information only to other authorised persons
- Exchange passwords only when absolutely necessary. When exchanging them in-person isn't possible, employees should prefer the phone instead of email, and only if they personally recognize the person they are talking to.
- Provide Computer and device login passwords to ECKA Management.

TRANSFER DATA SECURELY

Transferring data introduces security risk. Employees must:

- Avoid transferring sensitive data (e.g. child information, employee records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, we request employees to ask the ECKA office for help.
- Ensure that the recipients of the data are properly authorized people.

- Report scams, privacy breaches and hacking attempts

ECKA management need to know about scams, breaches and malware so they can better protect our infrastructure. For this reason, we advise our employees to report perceived attacks, suspicious emails or phishing attempts as soon as possible to the ECKA administration office. ECKA management must investigate promptly, resolve the issue and send an association wide alert when necessary.

ADDITIONAL MEASURES

To reduce the likelihood of security breaches, we also instruct our employees to:

- Turn off their screens and lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible to Management
- Change all account passwords at once when a device is stolen and report any lost or stolen device to Management.
- Report a perceived threat or possible security weakness in our systems.
- Refrain from downloading suspicious, unauthorized or illegal software on ECKA equipment.
- Avoid accessing suspicious websites.

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.

DISCIPLINARY ACTION

- First-time, unintentional, small-scale security breach: We may issue a verbal warning and train the employee on security.
- Intentional, repeated or large scale breaches (which cause severe financial or other damage): We will invoke more severe disciplinary action up to and including termination.

We will examine each incident on a case-by-case basis.

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 Eureka Community Kindergarten Association Inc. (ECKA) ICT facilities

Student's name:_____

Date of placement: _____

I,_____ , am a parent/guardian of

_____

I have read the Eureka Community Kindergarten Association Inc. (ECKA) *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 Eureka Community Kindergarten Association Inc. (ECKA) provides no censorship of access to ICT facilities.

_____ _____

Signature (student) Date

_____ _____

Signature (parent/guardian) Date