INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) POLICY

Best Practice – Quality Area 7

To view the full version of this policy (including attachments); please speak to the staff at your early learning service.

Uniting Victoria and Tasmania Limited is the Approved Provider of children's services known in these policies as Uniting Early Learning.

Overarching Policy Statement:

The *Keeping Children Safe Policy* of the Uniting Church in Australia Synod of Victoria and Tasmania (refer to *Sources*) is the overarching whole of church policy to be implemented by individuals and entities involved with or connected to the Uniting Church. All children who are involved in any of the Church's activities, events or programs have a right to feel and be safe. The Church is committed to provide safe environments where children are cared for, respected, nurtured and sustained.

Policy statement

Uniting Early Learning 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.

Purpose

This policy provides guidelines to ensure that all users of information and communication technology (ICT) at Uniting Early Learning:

- 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;*
- that only 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.

Summary of Procedures relating to this Policy

This policy and related procedures 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 including Facebook and Twitter
- 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.

It is everyone's responsibility at the service to be aware of and practice responsible use of all ICT, including maintenance of appropriate security measures around electronic data. With this in mind, suitable ICT facilities need to be available to enable educators and staff to effectively manage and operate the service.

Attachments 3 and 4 contain detailed information relating to procedures for use of ICT at the service, and Guiding Principles for security of information systems. Attachment 5 contains a sample Authorised User Agreement form for the use of staff.

Scope

This policy applies to the Approved Provider, Nominated Supervisor, Certified Supervisor, educators, staff, students on placement and volunteers at Uniting Early Learning.

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.

The responsibilities of each party listed in the previous paragraph are noted at Attachment 1.

Background and Legislation

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.

Attachment 2 contains a list of the legislation and sources relevant to this policy, including Acts and Regulations.

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
- helpdesk support.

The purpose of this support is to:

- establish ICT infrastructure to assist educators in the development and exchange of learning materials, and in recording children's learning
- contribute to the professional development of educators, 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).

Evaluation

In order to assess whether the goals 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

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.

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).

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.

Spam: Unsolicited and unwanted emails or other electronic communication.

USB interface: Universal Serial Bus (USB) is a widely used interface for attaching devices to a host computer. PCs and laptops have multiple USB ports that enable many devices to be connected without rebooting the computer or turning off the USB device.

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

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.

Authorisation

This policy was adopted by Uniting Victoria and Tasmania Limited on: 01/01/2017

Review date: December 2017

This Policy should be read in conjunction with:

- *Code of Conduct Policy*
- *Complaints and Grievances Policy*
- *Educational Program and Practice Policy*
- *Enrolment and Orientation Policy*
- *Governance and Management of the Service Policy*
- *Occupational Health and Safety Policy*
- *Privacy and Confidentiality Policy*
- *Staffing Policy*