Information and Communication Technology (ICT) Policy

Harrietville Bush Kinder

Best Practice – Quality Area 7

PURPOSE

This policy will provide guidelines to ensure that all users of information and communication technology (ICT) at Harrietville Bush Kindergarten or on behalf of Harrietville Bush Kinder:

- 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*
- 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.

POLICY STATEMENT

1. VALUES

Harrietville Bush Kindergarten 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, Service Manager, Certified Supervisor, educators, staff, students on placement and volunteers at Harrietville Bush 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 – 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 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: Leadership and Service Management - Standard 7.3: Administrative systems enable 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.

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 educators/families are not using personal recording devices to document children.
- 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
- considering encryption (refer to *Definitions*) of data for extra security
- 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, 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 (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 3 – Parent/guardian authorisation for under-age access to the Harrietville Bush Kindergarten ICT facilities).

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
- completing the authorised user agreement form (see Attachment 4)
- keeping allocated passwords secure, including not sharing passwords and logging off after using a computer
- maintaining the security of ICT facilities belonging to Harrietville Bush Kindergarten
- 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

- if using mobile phones or recording devices whilst documenting children's learning, deleting photos and videos immediately after
- 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
- signing an acknowledgement form upon receipt of a USB or portable storage device (including a laptop) (refer to Attachment 4 – Authorised user agreement)
- 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
- 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 the service
- Attachment 2: Guiding principles for security of information systems
- Attachment 3: Parent/guardian authorisation for under-age access to the Harrietville Bush Kindergarten ICT facilities
- Attachment 4: Authorised user agreement

AUTHORISATION

This policy was adopted by the Approved Provider of Harrietville Bush Kindergarten on 19/06/2024.

REVIEW DATE: June 2026