



INFORMATION COMMUNICATION TECHNOLOGY POLICY

Policy Number: G-1-07-2012	Version: 7
Responsible Person: BoG -Chair	Approved by BoG on: 12-06-2023
	Review date: 05- 2024

Quality Area 7

Purpose

This policy will provide guidelines to ensure that all users of information and communication technology (ICT) at Hampton Park Community House or on behalf of Hampton Park Community House:

- understand and follow procedures to ensure the safe and appropriate use of ICT Hampton Park Community House, including maintaining secure storage of information
- take responsibility to protect and maintain privacy in accordance with HPCH's *Privacy and Confidentiality Policy*
- are aware that only those persons authorised by the approved provider are permitted to access ICT at HPCH
- understand what constitutes illegal and inappropriate use of ICT facilities and avoid such activities.
- understand and follow professional use of interactive ICT platforms, such as social media (*refer to Definitions*) and other information sharing platforms (*refer to Definitions*).

Policy Statement

Values

- Hampton Park Community House is committed to:
- professional, ethical and responsible use of ICT at HPCH
- providing a safe workplace for management, educators, staff and others using HPCH's ICT facilities and information sharing platforms
- safeguarding the privacy and confidentiality of information received, transmitted or stored electronically
- ensuring that the use of HPCH'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 HPCH.

Scope

This policy applies to the BoG -approved provider or persons with management or control, nominated supervisor, persons in day-to-day charge, early childhood teachers, educators, staff, students, volunteers, at Hampton Park Community House. **This policy does not apply to children.** Refer: eSafety Policy

Responsibilities

Approved provider and persons with management or control	Nominated supervisor and persons in day-to-day charge	Early childhood teacher, educators and all other staff	Parents/guardians	Contractors, volunteers and students
--	---	--	-------------------	--------------------------------------

R indicates legislation requirement, and should not be deleted

Ensuring all records and documents are maintained and stored in accordance with *Regulations 181 and 183 of the Education and Care Services National Regulations 2011*

R	√	√		√
R	√			

Ensuring HPCH complies with the requirements of the *Health Privacy Principles* as outlined in the *Health Records Act 2001*, the *Information Privacy Principles* as outlined in the privacy and data protection act 2014 (Vic) and, where applicable, the *Australia Privacy Principles* as outlined in the *Privacy Act 1988 (Cth)* and the *Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)*, by taking proactive steps to establish and maintain internal practices, procedures, and systems that ensure compliance with privacy legalisations including:

- identifying the kind of personal, sensitive, and health information that will be collected from an individual or a family
- communicating the reason why personal, sensitive, and health information is being collected, and how it will be stored, used, and disclosed, and managed



and are provided with HPCH's privacy statement (refer to Attachment 4) and all relevant forms

- communicating how an individual or family can access and/or update their personal, sensitive, and health information at any time, to make corrections or update information (refer to Attachment 4)
- communicating how an individual or family can complain about any breaches of the privacy legislation, and how HPCH will deal with these complaints

Ensuring a copy of this policy, including the Privacy Statement, is provided to all stakeholders, is prominently displayed at HPCH and/or electronically accessible, is up to date and available on request

Reading and acknowledging they have read the *Privacy and Confidentiality Policy*, including the Privacy Statement (refer to Attachments 3 & 4 as applicable)

Maintaining the management of privacy risks at each stage of the information lifecycle, including collection, use, disclosure, storage, destruction or de-identification

Protecting personal information from misuse, interference, loss and unauthorised access, modification or disclosure, as well as unauthorised access, modification or disclosure.

Identifying and responding to privacy breaches, handling access and correction requests, and receiving and responding to complaints and inquiries

Providing regular staff training and information on how the privacy legislation applies to them and HPCH

Ensuring appropriate supervision of staff who regularly handle personal, sensitive, and health information

Ensuring that personal, sensitive, and health information is only collected by lawful and fair means, and is accurate and complete

Ensuring parents/guardians know why personal, sensitive and health information is being collected and how it will be used,

R	√			
R	√	√	√	√
R	√	√		
R	√	√		
R	√			
R	√			
R	√	√		
R	√	√		
R	√	√		

disclosed and managed and are provided with HPCH's Privacy Statement (*refer to Attachment 4*) and all relevant forms

Ensuring that an individual or family can have access to their personal, sensitive and health information at any time, to make corrections or update information (*refer to Attachment 4*)

Providing adequate and appropriate secure storage for personal, sensitive, and health information collected by HPCH, including electronic storage (*refer to Attachment 2*)

Ensuring that records and documents are kept in accordance with *Regulation 183*

Notifying an individual or family if HPCH receives personal sensitive and health information about them from another source as soon as practicably possible

Ensuring that if personal, sensitive and health information needs to be transferred outside of Victoria, that the individual or family that it applies to has provided consent, or if the recipient of the personal information is subject to a law or binding scheme.

Ensuring the unique identifiers are not adopted, used or disclosed unless lawfully required to (*refer to Attachment 2*)

Ensuring reasonable steps to destroy personal and health information and ensure it is de-identified if the information is no longer required for any purpose as described in *Regulations 177, 183, 184* (*refer to Attachment 2*)

Complying with the Notifiable Data Breaches Scheme (*refer to Definitions*) which imposes an obligation to notify individual whose personal information is in a data breach that is likely to result in serious harm.

Developing a data breach (*refer to Sources*) response plan that sets out the roles and responsibilities involved in managing a data breach, the steps taken if a data breach occurs (*refer to Sources*) and notifying the *Office of the Australian Information Commission* as appropriate.

Promoting awareness and compliance with the Child Safe Standards (*refer to Definitions*), and disclosing information to

R	√	√	√	√
R	√			
R	√	√		
R	√			
R	√			
R	√			
R				
R	√			
R				
R	R	R		



promote the wellbeing and safety of a child or group of children

Providing notice to children and parents/guardians when photos/video recordings are going to be taken at HPCH

Ensuring that images of children are treated with the same respect as personal information, and as such are protected by privacy laws in the same way

Ensuring the appropriate use of images of children, including being aware of cultural sensitivities and the need for some images to be treated with special care

Being sensitive and respectful to parents/guardians who do not want their child to be photographed or videoed

Being sensitive and respectful of the privacy of other children and parent/guardian in photographs/videos when using and disposing of these photographs/videos

Establishing procedures to be implemented if parents/guardians request that their child's image is not to be taken, published, or recorded, or when a child requests that their photo not be taken

Including a confidentiality clause relating to appropriate information handling in the agreement or contract between a photographer and HPCH.

√	√	√		√
R	R	R	R	R
√	√	√	√	√
R	√	√	√	√
R	√	√		
R	√			√

Child Information and Family Violence Sharing Scheme

Ensuring information sharing procedures abide by the *Child Information Sharing Scheme (CISS) Ministerial Guidelines and Family Violence Information Sharing (FVISS) Ministerial Guidelines (refer to Source)* and exercising professional judgment when determining whether the threshold for sharing is met, what information to share and with whom to share it (*refer to Attachment 7*)

Identifying which staff should be authorised point of contact in relation to the CISS and the FVISS (*refer to Definitions*)

Ensuring the authorised point of contact undertakes appropriate training and is aware of their responsibilities

R	R	R		
R	√			
R	√			



under the CISS and FVISS (*refer to Definitions*)

Being aware of who the point of contact at HPCH under the CISS and FVISS, and supporting them (if applicable) to complete the threshold test (*refer to Attachment 7*)

Communicating to staff about their obligations under the Information Sharing Schemes, and ensure they have read this policy

Providing opportunities for identified ISE staff to undertake the appropriate Information Sharing and MARAM online Learning System training (*refer to Sources*)

Engaging in training about Information Sharing and MARAM online Learning System training (*refer to Sources*)

Ensuring information sharing procedures are respectful of and have regard to a child's social, individual, and cultural identity, the child's strengths and abilities, and any vulnerability relevant to the child's safety or wellbeing

Ensuring any requests from ISE's are responded to in a timely manner and provide relevant information if the requirements for sharing under CISS or FVISS (*refer to Definitions*) are met (*refer to Attachment 7*)

Promoting a child's cultural safety and recognise the cultural rights and familial and community connections of children who are Aboriginal, Torres Strait Islander or both when sharing information under the CISS and FVISS (*refer to Definitions*)

Giving precedence to the wellbeing and safety of a child or group of children over the right to privacy when sharing information under the CISS and the FVISS (*refer to Definitions*)

Ensuring confidential information is only shared to the extent necessary to promote the wellbeing or safety of a child or group of children, consistent with the best interests of that child or those children

Maintaining record keeping processes that are accurate and complete as set by *Child Wellbeing and Safety (Information Sharing) Regulations* concerning both written and verbal sharing of information and or complaints (*refer to Attachment*

	R	R		
R	√			
R	√			
√	√	√		
√	√	√		
R	R	R		
R	R	R		
R	R	R		
R	R	R		

7)

Ensuring actions are taken when an ISE becomes aware that information recorded or shared about any person is incorrect, and is corrected in a timely manner

Working collaboratively with services that are authorised and skilled (including those located within The Orange Door) to determine appropriate actions and promote collaborative, respectful practice around parent/guardian and children

Seeking and taking into account the views and wishes of the child and the child's relevant family members, if it is appropriate, safe and reasonable to do so when sharing information under the CISS and the FVISS (*refer to Definitions*)

R	R	R		
R	R	R		
R	R	R		

Procedures

Refer to *Attachment 1* for the following procedures:

- Email usage
- Digital storage of personal and health information
- Data back up
- Password management

Background and Legislation

Background

- 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.

- The Victorian Government funds the State Library Victoria to deliver the Kindergarten IT Program, which provides the following services to eligible organisations:

Internet connectivity for kindergartens (data connection only)

Twenty email addresses per kindergarten

User support for general computer and Microsoft software enquiries

Web hosting options

Coordinated IT Training for eligible services including privacy and cyber safety training

Providing advice for kindergartens purchasing new computers with the option to supply and install (kindergartens meet the purchase and installation costs)

Repair of computer hardware that was provided by the Department of Education and Training through the Kindergarten IT Project roll-out

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)

Crimes Act 1958 (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)

Cybercrime Act 2001 (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)

Protected Disclosure Act 2012 (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: www.legislation.vic.gov.au

Commonwealth Legislation – Federal Register of Legislation: www.legislation.gov.au



Definitions

The terms defined in this section relate specifically to this policy.

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 recipient 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 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:

Content: being exposed to illegal, inappropriate or harmful material

Contact: being subjected to harmful online interactions with other users (including bullying)

Conduct: personal online behaviour that increases the likelihood of, or causes, harm.

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.

Information sharing platforms: Describes the exchange of data between various organisations, people and technologies This can include but no limited to Dropbox, Google Drive, Sharepoint, Skype for Business, One Drive

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.



PDA (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.

Social Media: A computer-based technology that facilitates the sharing of ideas, thoughts, information and photos through the building of virtual networks and communities. Examples can include but not limited to, Facebook, YouTube, WhatsApp, Facebook Messenger, TikTok and Instagram

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.

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.

Sources and Related Policies

Sources

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
- Compliments and Complaints
- Curriculum Development
- Enrolment and Orientation
- Governance and Management of HPCH
- Occupational Health and Safety
- Privacy and Confidentiality
- Staffing

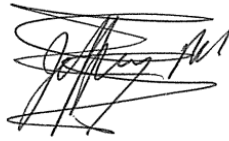


Evaluation

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 HPCH's policy review cycle, or as required
- notifying all stakeholders affected by this policy at least 14 days before making any significant changes to this policy or its procedures, unless a lesser period is necessary due to risk (*Regulation 172 (2)*)

Authorisations:



Signature BoG Chair:

Date: 12-06-2023

