

Staffing: Safe use of digital technologies and online environments policy

Policy Number: CS-18-08-2025
Responsible Person: BoG Chair

Version: 1 (New)
Approved by BoG on: 18-08-2025
Review date: 07-2026

Purpose

This policy will provide clear guidelines to support the safe use of digital technologies and online environments at Hampton Park Community House (HPCH) by ensuring:

- understand and follow procedures to ensure the safe and appropriate use of digital technologies Hampton Park Community House, including maintaining secure storage of information
- take responsibility to protect and maintain privacy in accordance with the service's Privacy and Confidentiality Policy
- promote a child safe culture when it comes to taking, use, storage and destruction images or videos of children
- are aware that only those persons authorised by the approved provider are permitted to access digital devices at the service
- understand what constitutes illegal and inappropriate use of digital devices and avoid such activities.
- understand and follow professional use of interactive digital technologies 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:

- providing a safe environment through the creation and maintenance of a child safe culture, and this extends to the safe use of digital technologies and online environments
- professional, ethical and responsible use of digital technologies at the service
- providing a safe workplace for management, educators, staff and others using the service's digital technologies and information sharing platforms



- the rights of all children to feel safe, and be safe at all times
- safeguarding the privacy and confidentiality of information received, transmitted or stored electronically
- ensuring that the use of the service's digital technologies complies with all service policies and relevant government legislation

Scope

This policy applies to the approved provider, persons with management or control, nominated supervisor, persons in day-to-day charge, early childhood teachers, educators, staff, students, volunteers, parents/guardians, children, and others attending the programs and activities of Hampton Park Community House (HPCH), including during offsite excursions and activities.

This policy applies to the approved provider or persons with management or control, nominated supervisor, persons in day-to-day charge, early childhood teachers, educators, staff, students, volunteers, at HPCH. This policy does not apply to children. Where services are using digital technologies within their educational programs, they should develop a separate policy concerning the use of digital technologies by children (refer to eSafety Policy).

This policy applies to all aspects of the use of digital technologies including:

- desktop top computers, laptops/notebooks, tablets, iPads, smartphones and smart devices
- copying, saving or distributing files
- electronic mail (email)
- file sharing
- file storage (including the use of end point data storage devices – refer to Definitions)
- file transfer/Cloud
- instant messaging
- internet usage
- portable communication devices including mobile and cordless phones.
- printing material
- social media (refer to Definitions)
- streaming media
- subscriptions to list servers, mailing lists or other like services
- video conferencing
- weblogs (blogs)

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					
1.Ensuring that the use of the service's digital technologies complies with all relevant state and federal legislation (refer to Legislation and standards), and all service policies (including Privacy and Confidentiality Policy, eSafety for Children and Code of Conduct Policy)	R	☒	☒	☒	☒
2.Ensuring staff understand how to actively supervise children while using digital technologies	R	R			
3.Undertaking risk assessments (refer to Sources) identifying the service's digital technologies practices, identify strengths and areas for improvement	R	☒	☒		☒
4.Obtaining parent/guardian consent before taking, retaining, or sharing images and videos of children (refer to Enrolment and Orientation and Privacy and Confidentiality policy)	R	☒	☒		☒
5.Asking children for permission before taking photos or videos and explain how these will be used	☒	☒	☒		☒
6.Regularly monitoring use of service-issued electronic devices to ensure that they are being used appropriately	R	☒			
7.Ensuring capturing, using, storing, and disposing of images, videos, and audio recordings of children are in line with privacy requirements (refer to Privacy and Confidentiality policy)	R	☒	☒		☒
8.Ensuring oversight and control of who has access to images (digital and hard copy) of children, including the movement of these onto devices and platforms	R	R			
9.Ensuring staff do not transfer images of children to their own account or device either directly or via the cloud, for example, to post images or videos on social media or other applications / software platforms that were not its intended purpose.	R	R			

10.Ensuring surveillance and monitoring devices are in line with privacy requirements	R	☑			
11.Ensuring that the Safe Use of Digital Technologies and Online Environments Policy and procedures are implemented, the appropriate risk assessments and action plans are completed, and all identified actions are taken to minimise the risks to children's health and safety	R	R	☑		☑
12.Promoting a culture of child safety and wellbeing that underpins all aspects of the service's operations (including online learning environments), to reduce risk to children (including the risk of abuse)	R	☑	☑		☑
13.Ensuring the safe use of digital technologies, including wearable devices, networks, platforms, apps, and networked toys within the service, and that they are password protected and in line with privacy principle (refer to Privacy and Confidentiality policy)	R	R	☑		☑
14.Ensuring that person who is providing education and care and working directly with children (refer to Definitions) do not carry their personal electronic devices (refer to Definitions) while providing education and care to children, except for authorised essential purposes (refer to Definitions)	R	☑	☑	☑	☑
15.Ensuring authorisation is documented for when a person who is providing education and care and working directly with children (refer to Definitions) may need to continue to carry their personal electronic device (refer to Definitions) while educating and care for children (example: medical conditions) (Refer to Attachment 6)	R	☑			
16.Ensuring a suitable log is maintained to record all essential purpose authorisations forms, that all logs are stored securely and available at the service for authorised officers to inspect	R	☑			
17.Maintaining a log for third party professionals attending the service and working directly with children (such as an allied health or inclusion professional) that they are using business or organisation issued devices are used only for work purposes (and not personal use)	R	R	☑		☑
18.Providing a secure place for persons who are providing education and care, and working directly with children (refer to Definitions), to store their personal digital devices while they are working with children	☑	☑			
19.Ensuring teachers and educators do not use personal devices for multi-factor authentication to access and use Arrival while providing education and care and working directly with children.	R	R	R		R
20.Ensuring that personal devices are only accessed by teachers, educators and other staff when they are not providing education and care or working directly with children. Examples could include:	R	R	R		R

- while taking a scheduled break from work, such as a lunch or tea break - during planning time - during administrative activities. Staff can also carry and use personal electronic devices that: - cannot take images or videos, and - are not storage and file transfer media.					
21.Undertaking risk assessments identifying whether personal devices (including wearable devices) can be used at the service and in what circumstances	R	R	☑		☑
22.Managing inappropriate use of digital technologies as described in Attachment 2	R	☑			
23.Providing suitable digital technologies facilities to enable early childhood teachers, educators and staff to effectively manage and operate the service	R	☑			
24.Ensuring there are sufficient service-issued devices available when programs are delivered outside the approved service premises (such as bush, beach or other nature programs)	R	R			
25.Ensuring that personal devices that take and store images are only used for emergency during excursions and regular outings, and that essential purposes authorisation (refer to Attachment 6) documentation is completed prior to excursions and regular outings	R	R	☑	☑	☑
26.Ensuring restricted persons (refer to Definitions) do not use their personal devices to record images of children when providing education and care and working directly with children	R	☑	☑	☑	☑
27.Ensuring parents/guardians do not use their personal devices to record images of children, this includes during service events	R			☑	
28.Ensuring third party professional attending the service and working directly with children (such as an allied health or inclusion professional) only use devices that is issued by their business or institution; and is used only for work purposes (and not personal use)	R	☑	☑		☑
29.Authorising the access of early childhood teachers, educators, staff, volunteers and students to the service's digital technologies facilities, as appropriate	R	R			
30.Providing clear procedures and protocols that outline the parameters for use of the service's digital technologies facilities both at the service and when working from home (refer to Attachment 1)	☑	☑			
31.Embedding a culture of awareness and understanding of security issues at the service	R	☑	☑	☑	☑

32. Never posting online photos or videos of children who: - Are subject to child protection, family court, or criminal proceedings - Are experiencing family violence or need to remain anonymous - Have parents concerned about their child's digital footprint	R	☒	☒	☒
33. Ensuring that effective financial procedures and security measures are implemented where transactions are made using the service's digital technologies facilities, e.g. handling fees, invoice payments, and using online banking	R	☒		
34. Ensuring that the service's computer software and hardware are purchased from an appropriate and reputable supplier	☒	☒		
35. Identifying the need for additional password-protected email accounts for management, early childhood teachers, educators, staff and others at the service, and providing these as appropriate	☒	☒		
36. Removing access on online platforms for staff, parents/guardians and others when they leave the service	R	R		
37. Identifying the training needs of early childhood teachers, educators and staff in relation to digital technologies, and providing recommendations for the inclusion of training in digital technologies in professional development activities	☒	☒		
38. Ensuring regular backup of critical data and information at the service (refer to Attachment 1)	☒	☒	☒	
39. Ensuring secure storage of all information (including images and videos of children) at the service, including backup files (refer to Privacy and Confidentiality Policy)	R	☒	☒	
40. Adhering to the requirements of the Privacy and Confidentiality Policy in relation to accessing information on the service's computer/s, including emails	R	R	R	
41. Considering encryption (refer to Definitions) of data for extra security	☒	☒		
42. Ensuring that reputable anti-virus and firewall software (refer to Definitions) are installed on service computers, and that software is kept up to date	☒	☒		
43. Developing procedures to minimise unauthorised access, use and disclosure of information and data, which may include limiting access, passwords, multifactor authentication and encryption (refer to Definitions)	R	☒		
44. 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)	R	☒		

45.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	R	☑			
46.Being aware of the requirements and complying with this policy	☑	☑	☑	☑	☑
47.Appropriate use of endpoint data storage devices (refer to Definitions) by digital technologies users at the service	R	☑	☑	☑	☑
48.Ensuring that all material stored (including images and videos of children) on endpoint data storage devices is also stored on a backup drive, and that both device and drive are kept in a secure location	R	☑	☑		☑
49.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 5).	R	☑			☑
50.Developing guidelines on the use of Artificial Intelligence (AI) refer to Attachment 7 (if applicable to the service)	☑	☑			
51.Providing authorisation to early childhood teachers, educators and staff to be social media representatives for HPCH (refer to Attachment 3)	☑	☑			
52.Complying with all relevant legislation and service policies, protocols and procedures, including those outlined in Attachments 1	R	R	R	R	R
53.Reading and understanding what constitutes inappropriate use of digital technologies (refer to Attachment 2)	☑	☑	☑	☑	☑
54.Ensuring that if working from home, the service device does not leave the service unless they contain no images of children (refer to Attachment 1 and 4)	R	R	☑		☑
55.Completing the authorised user agreement form when using service devices outside the service (refer to Attachment 4)	☑	☑	☑		☑
56.Maintaining the security of digital technologies facilities belonging to Hampton Park Community House and keeping allocated passwords secure, including not sharing passwords and logging off after using a computer	R	R	R	☑	R
57.Accessing accounts, data or files on the service's computers only where authorisation has been provided		☑	☑		☑
58.Co-operating with other users of the service's digital technologies to ensure fair and equitable access to resources	☑	☑	☑		☑
59.Obtaining approval from the approved provider before purchasing licensed computer software and hardware		☑	☑		
60.Ensuring no illegal material is transmitted at any time via any digital technology medium (refer to Attachment 2)	R	☑	☑	☑	☑

61.Using the service's email, messaging and social media (refer to Definitions) facilities for service-related and lawful activities only (refer to Attachment 2)	☑	☑	☑	☑	☑
62.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		☑	☑		☑
63.Notifying the approved provider of any damage, faults or loss of endpoint data storage devices		R	R		R
64.Notifying the approved provider and/or nominated supervisor immediately if they observe any inappropriate use of personal or service issued electronic devices at the service			☑	☑	☑
65.Signing an acknowledgement form upon receipt of a USB or portable storage device (including a laptop) (refer to Attachment 4)		☑	☑		☑
66.Restricting the use of personal mobile phones to rostered breaks, and only used in areas outside of spaces being utilised for education and care of children	☑	☑	☑	☑	☑
67.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)	☑	☑	☑		☑
68.Ensuring electronic devices and files containing images and information about children and families are kept secure at all times (refer to Privacy and Confidentiality Policy)	R	R	R		R
69.Responding to a privacy breach in accordance with Privacy and Confidentiality policy.	R	☑			
70.Complying with the appropriate use of social media (refer to Definitions) platforms (refer to Attachment 3)	☑	☑	☑		☑
71.Always complying with this policy to protect the privacy, confidentiality and interests of Hampton Park Community House employees, children and families	R	R	R		R

Background

The digital technology landscape is continually evolving. Early childhood and community services now rely on fixed, wireless and mobile technologies for communication, service management, learning, and stakeholder engagement. These tools offer efficiency and access, but also introduce legal, ethical and operational responsibilities relating to privacy, security, child safety and staff conduct.



As a community provider, Hampton Park Community House (HPCH) engages a specialist, organisation-wide IT support service (Razornet Technologies) to manage and secure our technology environment across all program areas. This partnership covers network and endpoint security, device lifecycle management, data backup and recovery, identity and access management (including MFA), patching and monitoring, and rapid incident response. Where Department-funded programs exist (e.g., sector supports available to some kindergarten services), they are considered supplementary to HPCH's primary specialist IT arrangements.

HPCH adopts a proactive risk-management approach to digital technologies. We identify hazards, analyse and evaluate risks, implement controls (technical, administrative and behavioural), and monitor their effectiveness through audits, training and incident review. Particular attention is paid to risks amplified by online platforms and AI-enabled tools (e.g., connected toys and apps), including potential vulnerabilities in Wi-Fi networks and unauthorised audio/video capture.

All use of digital technologies at HPCH is governed by applicable Commonwealth and Victorian legislation (privacy, records, copyright, cybercrime, OHS, anti-discrimination and sexual harassment), as well as our internal policies (Privacy and Confidentiality, Code of Conduct, Child Safe Environment and Wellbeing, social media, and related procedures). Inappropriate or unlawful use includes (but is not limited to) accessing or sharing illegal or offensive material, harassment (including sexual harassment and stalking), defamation, copyright infringement, privacy breaches and other illegal activities.

HPCH complies with the National Model Code expectations for early childhood education and care settings regarding images and recordings of children. Only service-issued devices are to be used for capturing images/video; exceptions for personal devices are tightly controlled, documented and risk-assessed for essential purposes only. Strict controls apply to the storage, access, retention and disposal of any images or recordings to protect children's privacy and maintain community trust.

Continuous improvement is embedded in our governance, via the Governance & Policy sub-committee, we review risks and controls on a quarterly cycle, update procedures as technology and threats evolve, provide regular staff training, and communicate expectations to volunteers, contractors and families. This demonstrates active consideration of digital risks and supports compliance with NQS Quality Area 7 (Governance and Leadership).

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.

Artificial intelligence (AI): An engineered system that generates predictive outputs such as content, forecasts, recommendations, or decisions for a given set of human defined objectives or parameters without explicit programming. AI systems are designed to operate with varying levels of automation.

AI Tools: Software, platforms, devices, or apps powered by AI, including chatbots, voice assistants, content-sorting algorithms, and AI-enabled toys or applications.

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).

Essential purposes: The use and / or possession of a personal electronic device may be authorised for purposes other than taking images or recording videos of children include:

- communication in an emergency situation involving a lost child, injury to child or staff member, or other serious incident, or in the case of a lockdown or evacuation of the service premises
- personal health requirements, e.g. heart or blood sugar level monitoring
- disability, e.g. where a personal electronic device is an essential means of communication for an educator or other staff member
- family necessity, e.g. a worker with an ill or dying family member
- technology failure, e.g. when a temporary outage of service-issued electronic devices has occurred
- local emergency event occurring, to receive emergency notifications through government warning systems, for example, bushfire evacuation text notification.

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.

Generative artificial intelligence (AI): A branch of AI that develops generative models with the capability of learning to generate novel content such as images, text, and other media with similar properties as their training data.

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

Illegal content: Illegal content includes:

- images and videos of child sexual abuse
- content that advocates terrorist acts
- content that promotes, incites or instructs in crime or violence
- footage of real violence, cruelty and criminal activity.

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's (Personal Digital Assistants): A handheld computer for managing contacts, appointments and tasks. PDA's typically include a name and address database, calendar, to-do list and note taker. Wireless PDA's 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.



Person who is providing education and care and working directly with children: In the context of this policy a person includes:

- teachers and educators, including casual and agency staff
- students attending the service as part of a practicum and representatives of tertiary providers who attend the service to assess students
- volunteers, including parent volunteers
- any third parties delivering programs or incursion activities to children in a service, whether paid or unpaid
- allied health and inclusion professionals attending a service to observe, assess or work with a child at the service
- mentors or coaches attending the service to support teachers or educators working with children or providing education and care
- preschool field officers
- primary school teachers attending a service as part of a school transition program.

If a third-party professional attending a service and working directly with children (such as an allied health or inclusion professional) needs to use a device (for example, to undertake an assessment or take notes) they can use a device that is:

- issued by their business or institution; and
- used only for work purposes (and not personal use).

Personal Electronic Device: cameras, wearables, such as camera glasses, USB drives, hard drives and cloud storage), which has the capability to capture and store images or video footage. These devices are not issued or controlled by the approved provider.

Phishing: Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.

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).

Ransomware: Ransomware is a type of malicious software that threatens to publish the victim's data or block access to it unless a ransom is paid.

Restricted persons: The National Model Code restrictions apply to any person who is providing education and care and working directly with children include:



- teachers and educators, including casual and agency staff
- students attending the service as part of a practicum and representatives of tertiary providers who attend the service to assess students
- volunteers, including parent volunteers
- any third parties delivering programs or incursion activities to children in a service, whether paid or unpaid
- allied health and inclusion professionals attending a service to observe, assess or work with a child at the service
- mentors or coaches attending the service to support teachers or educators working with children or providing education and care
- preschool field officers
- primary school teachers attending a service as part of a school transition program.

If a third-party professional attending a service and working directly with children (such as an allied health or inclusion professional) needs to use a device (for example, to undertake an assessment or take notes) they can use a device that is:

- issued by their business or organisation; and
- used only for work purposes (and not personal use).

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.

Vishing: Vishing is a form of phishing that uses the phone system or voice over internet protocol (VoIP) technologies. The user may receive an email, a phone message, or even a text encouraging them to call a phone number due to some discrepancy. If they call, an automated recording prompts them to provide detailed information to verify their account such as credit card number, expiration date or birthdate.

Sources and related policies

Sources

- Department of Education: Acceptable Use Policy, DE Information, Communications and Technology (ICT) Resources
- IT for Kindergartens: www.kindergarten.vic.gov.au
- ACECQA: National Model Code - Taking images in early childhood education and care
- ACECQA: Empowering children under 5 by asking them to give consent for photos or videos
- ACECQA: NQF Online Safety Guide Self and Risk Assessment Tool
- ACECQA: Consent and children's rights
- ACECQA: How do I manage a data breach?
- OAIC: Guidance on privacy and the use of commercially available AI products

Related Policies

- Child Safe Environment and Wellbeing
- Code of Conduct
- Compliments and Complaints
- Educational Program
- Enrolment and Orientation
- eSafety for Children
- Excursions, Regular Outings and Service Events
- Governance and Management of the Service
- In nature programs
- Occupational Health and Safety
- Privacy and Confidentiality
- Staffing

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
- 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)*).

Procedures

Refer to Attachment 1 for the following procedures

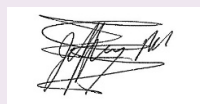
- Email usage
- Digital storage of personal and health information
- Data back up
- Password management

Attachments:

- Attachment 1: Procedures for use of digital technologies at the service
- Attachment 2: Unacceptable/inappropriate use of digital technologies
- Attachment 3: Social Media Guidelines
- Attachment 4: Authorised user agreement
- Attachment 5: Parent/guardian authorisation for under-age access to the HPCH digital technology facilities:
- Attachment 6: Essential purpose authorisations
- Attachment 7: Guidelines for the use of AI

Authorisations:

Signature of the Board Chair:



Date: 18-08-2025

ATTACHMENT 1. PROCEDURES FOR USE OF DIGITAL TECHNOLOGIES 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.
- Create an email signature that identifies employee name, title, service name, service phone number and address
- 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.
- Never send unauthorised marketing content or solicitation emails
- Be suspicious of phishing titles
- Always treat attachments as being infected. Never open Unsolicited emails with attachments unless you know it is safe to do so. If you do open an attachment that looks or acts suspicious, contact IT immediately.

Digital storage of personal and health information

- Digital records containing personal, sensitive and/or health information, or images of children must be password protected and 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).
- Digital records containing personal, sensitive and/or health information, or images of children may need to be removed from the service from time-to-time for various reasons, including for:
 - excursions and service events (refer to Excursions and Service Events Policy)
 - 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.

- Digital technology 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.

Backing up data

Data backup is the process of creating accessible data copies for use in the event of breach or loss.

- **Develop a written backup plan that identifies:**
 - What's being backed up - All emails, OneDrive data, SharePoint data
 - Where it's being backed up - Backup servers within Australia
 - How often backups will occur- Minimum of 1 time a day up to 3 times a day for some data
 - Who's in charge of performing backups- Razornet Technologies
 - Who's in charge of monitoring the success of these backups- Razornet Technologies
 - How will backup drives be stored securely - All backups are stored using industry standard security and encryption

HPCH has both onsite (for Server) or remote backup:

- Onsite backup
Onsite backups are done once per day and stored on a portable drive. Drive are replaced each week.
- Remote backup- cloud Microsoft 365 *SharePoint*
 - install the software (OneDrive) on every computer containing data that needs to be backed up,
 - set up a backup schedule, (Gold Standard 3 times per day) and
 - identify the *SharePoint* files and folders to be copied.

Password management

The effective management of passwords is the first line of defence in the electronic security of an organisation. Every ICT facility should have a password strategy in place as part of the overall security strategy. The technical considerations and principals outlined below are intended to be used as a guide for developing a password procedure.

Technical considerations include:

- a strong password should:
 - Be at least 8 characters in length
 - Contain both upper and lowercase alphabetic characters (e.g. A-Z, a-z)

- Have at least one numerical character (e.g. 0-9)
- Have at least one special character (e.g. ~!@#\$\$%^&*()_-=)
- always verify a user's identity before resetting a password
- change passwords when an employer leaves the service
- password rotation; changed every 90 days or less
- do not use automatic logon functionality
- use of account lockouts for incorrect passwords, with a limit of 5 or fewer bad attempts.

Users should always follow these principles:

- do not share passwords with anyone. If there is an issue that requires you to do so, remember to change the password immediately after the issue has been resolved.
- never use the same password for work accounts as the one you have for personal use (banking, etc.).
- do not write down passwords or include them in an email.
- do not store passwords electronically unless they are encrypted.
- never use the "remember password" feature on any systems; this option should be disabled
- Do not use the same password for multiple administrator accounts.

Working from home

When an approved provider, nominated supervisor, early childhood teachers, educators, other staff members or contractors are working from home they must:

- complete the authorised user agreement form (refer to Attachment 4)
- that images of children are not accessed, or transferred onto personal devices
- conduct a workstation assessment, taking reasonable care in choosing a suitable workspace, including ergonomics, lighting, thermal comfort, safety, and privacy
- ensure security and confidentiality of workspace, keeping private, sensitive, health information, planning, educational programs and children's records confidential and secure at all times
- keep allocated passwords secure, including not sharing passwords and logging off after using a computer
- adhere to the Privacy and Confidentiality Policy
- report breaches to privacy or loss of private, sensitive, and health information to nominated superiors as soon as practically possible.



ATTACHMENT 2. UNACCEPTABLE/INAPPROPRIATE USE OF DIGITAL TECHNOLOGY FACILITIES

Users of the digital technologies' facilities (and in particular, the internet, email and social media) provided by Hampton Park Community House 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 digital technology 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 digital technology 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 digital technology 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 [Service Name]
- conduct any outside business or engage in activities related to employment with another organisation
- play games
- use the facilities to assist any election campaign or lobby any government organisation
- exchange any confidential or sensitive information held by Hampton Park Community House 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.

Breaches of this policy

- Individuals who use digital technologies 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 digital technology 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 digital technology facilities restricted/denied.

Category 1: illegal — criminal use of material

This category includes but is not limited to:

- child abuse material offences relating to child pornography covered by the Crimes Act 1958 (Vic). 'Child abuse material' is defined in section 51A of the Crimes Act 1958 (Vic)
- objectionable material — offences relating to the exhibition, sale and other illegal acts relating to 'objectionable films' and 'objectionable publications' covered by the Classification (Publications, Films and Computer Games) (Enforcement) Act 1995 (Vic). Such material has or would attract a classification of X18+ (restricted) or RC (refused classification) under the Guidelines for Classification of Films 2012, Guidelines for the Classification of Computer Games 2012 or National Classification Code scheduled to the Classification (Publications, Films and Computer Games) Act 1995 (Cth)
- reckless or deliberate copyright infringement and any other material or activity that involves or is in furtherance of a breach of criminal law

Category 2: extreme — non-criminal use of material

This category includes non-criminal use of material that has or may attract a classification of RC or X18+ under the Guidelines for Classification of Films 2012, Guidelines for the Classification of Computer Games 2012 or National Classification Code scheduled to the Classification (Publications, Films and Computer Games) Act 1995 (Cth).

This includes any material that:

- depicts, expresses or otherwise deals with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that the material should not be classified
- describes or depicts in a way that is likely to cause offence to a reasonable adult or a person who is, or appears to be, a child under 18 (whether or not the person is engaged in sexual activity or not)
- promotes, incites or instructs in matters of crime or violence
- includes sexually explicit material that contains real depictions of actual sexual intercourse and other sexual activity between consenting adults

Category 3: critical — offensive material

This category includes other types of restricted or offensive material, covering any material that:

- has or may attract a classification of R18+ under the Guidelines for Classification of Films 2012, Guidelines for the Classification of Computer Games 2012 or National Classification Code scheduled to the Classification (Publications, Films and Computer Games) Act 1995 (Cth). Material may contain sex scenes and drug use that are high in impact
- includes sexualised nudity
- involves racial or religious vilification
- is unlawfully discriminatory
- is defamatory
- involves sexual harassment or bullying

Category 4: serious

- This category includes any use which is offensive or otherwise improper.
- The categories do not cover all possible breaches of this policy. Matters not covered by the above categories will be dealt with on an individual basis and on the relevant facts.



ATTACHMENT 3. SOCIAL MEDIA AND INFORMATION SHARING PLATFORM GUIDELINES

The following directives are essential to the safety and wellbeing of staff, children and their families, and to ensure that Hampton Park Community House (HPCH) operates in a professional and appropriate manner when using social media and/or information sharing platforms.

Staff must exercise extreme caution using digital technology facilities when accessing social media and/or information sharing platforms, whether in the workplace or relating to external events or functions involving HPCH.

It is a breach of confidentiality and privacy to make posts or comments about children, families, staff or management from HPCH on social media sites without consent or authorisation. It is also an offence under current legislation to record or use a visual image of a child, including transmitting the image on the internet, without the written consent of the child's parent.

Hampton Park Community House specifically requires that, unless you have the express permission, you:

- Do not video or photograph anyone, or post photos or personal details of other HPCH staff, children or families.
- Do not post photos or videos of Hampton Park Community House staff, children or families on your personal Facebook page, or otherwise share photos or videos of staff, children or families through social media;
- Do not create a Hampton Park Community House branded Facebook page, or other pages or content on social media that represents [Service Name], it's staff, children or families without authorisation from the Board of Governance (approved provider);
- Do not post anything that could embarrass or damage the reputation of HPCH, colleagues, children or families.

Staff must not:

- post or respond to material that is, or might be construed as offensive, obscene, fraudulent, defamatory, threatening, harassing, bullying, discriminatory, hateful, racist, sexist, infringes copyright, constitutes a contempt of court, breaches a Court suppression order, or is otherwise unlawful or inaccurate;
- make any comment or post any material that might otherwise cause damage to Hampton Park Community House's reputation or bring it into disrepute;
- imply that they are authorised to speak as a representative of [Service Name], or give the impression that the views expressed are those of [Service Name], unless authorised to do so
- use a [Service Name] email address or any Hampton Park Community House logos or insignia that may give the impression of official support or endorsement of personal comments;
- use the identity or likeness of another employee, contractor or other member of Hampton Park Community House;



- use or disclose any confidential information or personal information obtained in the capacity as an employee/contractor of Hampton Park Community House; or
- access and/or post on personal social media during paid workhours.

Personal use of social media

Hampton Park Community House recognises that staff may choose to use social media in their personal capacity. This policy is not intended to discourage nor unduly limit staff using social media for personal expression or other online activities in their personal life. Staff should be aware of and understand the potential risks and damage to Hampton Park Community House that can occur through their use of social media, even if their activity takes place outside working hours or on devices not owned by Hampton Park Community House.

If an individual can be identified as an employee of Hampton Park Community House on social media, that employee must:

- only disclose and discuss publicly available information;
- ensure that all content published is accurate and not misleading and, complies with all relevant policies of Hampton Park Community House
- expressly state on all postings (identifying them as an employee of [Service Name]) the stated views are their own and are not those of Hampton Park Community House;
- be polite and respectful to all people they interact with;
- adhere to the Terms of Use of the relevant social media platform/website, as well as copyright,
- abide by privacy, defamation, contempt of Court, discrimination, harassment and other applicable laws;
- ensure that abusive, harassing, threatening or defaming postings which are in breach of [Service Name] policies may result in disciplinary action being taken, even if such comments are made using private social networks outside of working hours.
- notify the approved provider or person with management or control if they become aware of unacceptable use of social media as described above.

Consequences of unacceptable use of social media

- HPCH will review any alleged breach of this policy on an individual basis. If the alleged breach is of a serious nature, the person shall be given an opportunity to be heard in relation to the alleged breach.
- If the alleged breach is clearly established, the breach may be treated as grounds for dismissal. In all other cases, the person may be subject to disciplinary action in accordance with [Service Name] Code of Conduct Policy.
- HPCH may request that any information contained on any social media platform that is in breach of this policy be deleted.
- HPCH may restrict an employee's access to social media on HPCH digital technology facilities or if they are found to have breached this policy or while HPCH investigates whether they have breached this policy.

ATTACHMENT 4. Authorised user agreement

Portable storage device (PSD) (including laptops)

I, _____,

acknowledge that I have received a PSD belonging to Hampton Park Community House

will ensure that the PSD:

- has no images of children
- is used for work-related purposes only
- is password-protected at all times
- will not be loaned to unauthorised persons
- will be returned to Hampton Park Community House on cessation of employment
- will notify the Domain Area Manager & IT support as soon as is practicable if the PSD is damaged, faulty or lost
- have read the Hampton Park Community House *Safe Use of Digital Technologies and Online Environment Policy* and agree to abide by the procedures outlined within.

Signature (authorised user)

Position

Date

Authorised by

Position

Date

**ATTACHMENT 5. PARENT/GUARDIAN AUTHORISATION FOR UNDER-AGE ACCESS TO THE
HAMPTON PARK COMMUNITY HOUSE'S DIGITAL TECHNOLOGY FACILITIES**

Student's name:

Date of placement:

I, _____, am a parent/guardian of

I have read the HPCH Safe Use of Digital Technologies and Online Environment Policy and
agree to the conditions of use of the service's digital technology facilities for the above-named student.
I also understand that HPCH provides no censorship of access to digital technology facilities.

Signature (student) Date

Signature (parent/guardian) Date

ATTACHMENT 6: ESSENTIAL PURPOSE AUTHORISATIONS FORM

Section 1: Personal Details

Staff Member Name:

Position:

Personal Device Type (e.g., Smartphone, Smart watch):

Date of use:

Section 2: Purpose

This form grants permission for the above-named staff member to use their personal device for the purposes of:

_____ at Hampton
Park Community House.

Section 3: Guidelines

1. Usage:

The National Model Code lists the following essential purposes for which the use or possession of a personal devices may be authorised where access does not impede the active supervision of children:

- communication in an emergency situation to ensure safety

involving a lost child, injury to child or staff member, or other serious incident

in the case of a lockdown or evacuation of the service premises

- personal health requirements
 - for example, heart or blood sugar level monitoring
- disability
 - for example, where a personal electronic device is an essential means of communication for an educator or other staff member
- family necessity



- for example, an early childhood staff member with an ill family member
- technology failure
 - for example, when a temporary outage of service-issued electronic devices has occurred
- during a local emergency event to receive emergency notifications. This could include government warning systems such as a bushfire evacuation text notification.

2. Professional Conduct:

- Staff must maintain a professional demeanour while using personal devices.
- Authorised essential purpose authorisations form must be on file and accessible at all times.
- Devices should not be used for personal matters during work hours, unless authorised.

Section 5: Acknowledgement and Agreement

I, _____ (Staff Member Name), acknowledge that I have read, understood, and agree to comply with the guidelines outlined in this form. I understand the importance of protecting the privacy and security of the children in my care and the potential repercussions of failing to adhere to these guidelines.

Staff Member Signature:

Date:

Domain Area Manager/Nominated Supervisor Name:

Domain Area Manager /Nominated Supervisor Signature:

Date: