

# INFORMATION & COMMUNICATION TECHNOLOGY

QUALITY AREA 7 | ELAA version 1.3

Working in partnership with Cancer Council Victoria, ELAA has aligned this policy to the key policies and guidelines of the Healthy Early Childhood Services Achievement Program.



## PURPOSE

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

- understand and follow procedures to ensure the safe and appropriate use of ICT Civic Kindergarten, 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, sharing and storing images or videos of children.
- are aware that only those persons authorised by the approved provider are permitted to access ICT at the service
- understand what constitutes illegal and inappropriate use of ICT facilities and avoid such activities.
- understand 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

Civic 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 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 ICT facilities complies with all service policies & relevant government legislation
- providing management, educators and staff with online information, resources and communication tools to support the effective operation of the service.

### SCOPE

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 Civic 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 (*refer to eSafety Policy*).

This policy applies to all aspects of the use of ICT 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
- weblogs (blogs)
- video conferencing

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
<b>R</b> indicates legislation requirement, and should not be deleted					
Ensuring that the use of the service’s ICT complies with all relevant state and federal legislation ( <i>refer to Legislation and standards</i> ), and all service policies ( <i>including Privacy and Confidentiality Policy and Code of Conduct Policy</i> )	<b>R</b>	√	√	√	√
Ensuring that only service-issued electronic devices should ever be used to take photos or record videos of children	√	√	√		√
Developing considerations for why a staff member may need to continue to carry their personal electronic device ( <i>refer to Definitions</i> ) while educating and care for children ( <i>refer to Attachment 6</i> )	√	√			
Ensuring that staff don’t not carry their personal electronic devices ( <i>refer to Definitions</i> ) while providing education and care to children, except for authorised essential purposes	√	√	√		√
Managing inappropriate use of ICT as described in <i>Attachment 2</i>	<b>R</b>	√			
Providing suitable ICT facilities to enable early childhood teachers, educators and staff to effectively manage and operate the service	√	√			
Ensuring staff do not use their personal devices to record images/videos of children	√	√			
Authorising the access of early childhood teachers, 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 both at the service and when working from home ( <i>refer to Attachment 1</i> )	√	√			
Embedding a culture of awareness and understanding of security issues at the service	<b>R</b>	√	√	√	√
Ensuring that effective financial procedures and security measures are implemented where transactions are made using the service’s ICT facilities, e.g. handling fees, invoice payments, and using online banking	<b>R</b>	√			
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, early childhood teachers, educators, staff and others at the service, and providing these as appropriate	√	√			
Identifying the training needs of early childhood teachers, educators and staff in relation to ICT, and providing recommendations for the inclusion of training in ICT in professional development activities	√	√			
Ensuring regular backup of critical data and information at the service ( <i>refer to Attachment 1</i> )	√	√	√		
Ensuring secure storage of all information (including images and videos of children) at the service, including backup files ( <i>refer to Privacy and Confidentiality Policy</i> )	<b>R</b>	√	√		
Adhering to the requirements of the <i>Privacy and Confidentiality Policy</i> in relation to accessing information on the service’s computer/s, including emails & Storypark.	<b>R</b>	<b>R</b>	<b>R</b>		

Ensuring that STV update reputable anti-virus and firewall software ( <i>refer to Definitions</i> ) 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 ( <i>refer to Definitions</i> )	R	√			
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 ( <i>refer to Definitions</i> )	R	√			
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	√			
Being aware of the requirements and complying with this policy	√	√	√	√	√
Appropriate use of endpoint data storage devices ( <i>refer to Definitions</i> ) by ICT users at the service	R	√	√	√	√
Ensuring that all material stored (including images and videos of children) on endpoint data storage devices and that the drive is kept in a secure location	R	√	√		√
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) ( <i>refer to Attachment 5</i> ).	R	√			√
Providing authorisation to early childhood teachers, educators and staff to be social media representatives for Civic Kindergarten ( <i>refer to Attachment 3</i> )	√	√			
Complying with all relevant legislation and service policies, protocols and procedures, including those outlined in <i>Attachments 1</i>	√	√	√	√	√
Reading and understanding what constitutes inappropriate use of ICT ( <i>refer to Attachment 2</i> )	√	√	√	√	√
Completing the authorised user agreement form ( <i>refer to Attachment 4</i> )	√	√	√		√
Maintaining the security of ICT facilities belonging to Civic Kindergarten and keeping allocated passwords secure, including not sharing passwords and logging off after using a computer	R	R	R	√	R
Accessing accounts, data or files on the service's computers only where authorisation has been provided		√	√		√
Ensuring no illegal material is transmitted at any time via any ICT medium ( <i>refer to Attachment 2</i> )	R	√	√	√	√
Using the service's email, messaging and social media ( <i>refer to Definitions</i> ) facilities for service-related and lawful activities only ( <i>refer to Attachment 2</i> )	√	√	√	√	√
Parent/guardians engaging in Information Technology Communication platforms such as WhatsApp, Facebook Messenger, SMS etc to communicate with Civic Kindergarten or parents/guardians (who attend Civic Kindergarten) is entirely at the parent/guardians discretion. These Information Technology Communication platforms are NOT governed or managed by Civic Kindergarten and its staff. <i>Refer to Code of Conduct Policy.</i>			√	√	√
Using endpoint data storage devices ( <i>refer to Definitions</i> ) supplied by KITP for the service for service-related business only, and ensuring that this information is protected from unauthorised access and use		√	√		√
Notifying the approved provider of any damage, faults or loss of endpoint data storage devices		R	R		R
Signing an acknowledgement form upon receipt of a USB or portable storage device (including a laptop) ( <i>refer to Attachment 4</i> )		√	√		√
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 by all educators.	√	√	√	√	√

Responding only to emergency phone calls when responsible for supervising children to ensure adequate supervision of children at all times ( <i>refer to Supervision of Children Policy</i> )	√	√	√		√
Ensuring electronic files containing information about children and families are kept secure at all times ( <i>refer to Privacy and Confidentiality Policy</i> )	R	R	R		R
Responding to a privacy breach in accordance with <i>Privacy and Confidentiality policy</i> .	R	√			
Complying with the appropriate use of social media ( <i>refer to Definitions</i> ) platforms ( <i>refer to Attachment 3</i> )	√	√	√		√
Complying with this policy at all times to protect the privacy, confidentiality and interests of Civic Kindergarten employees, children and families	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 provide IT support to kindergarten Early Years Management organisation and community-based kindergarten services that operate funded kindergarten programs.

Through the Kindergarten IT Program, the State Library Victoria 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 through the Kindergarten IT Project roll-out
- Provide web design support provided kindergarten meet the costs associated with this additional support.

Adopting the National Model Code is crucial for Early Childhood Education and Care (ECEC) services to ensure the safety and privacy of children. The National Model Code has been designed for voluntary adoption by ECEC services. Under the Code, only service-issued electronic devices should be used for taking photos or recording videos, thereby minimising the risk of unauthorised distribution of images. The Code states that clear guidelines are developed on carrying personal devices for specific essential purposes ensuring that any exceptions are justified and controlled. Additionally, implementing strict controls for storing and retaining images or recordings of children is vital to protect their privacy and prevent misuse of sensitive information. Adhering to these guidelines not only safeguards children but also fosters trust and transparency between ECEC services and families.

## 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](http://www.legislation.vic.gov.au)
- Commonwealth Legislation – Federal Register of Legislation: [www.legislation.gov.au](http://www.legislation.gov.au)



## DEFINITIONS

The terms defined in this section relate specifically to this policy. For regularly used terms e.g. Approved Provider, Nominated Supervisor, Notifiable Complaints, Serious Incidents, Duty of Care, etc. refer to the Definitions file of the PolicyWorks catalogue.

**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.

**Civic Kindergarten:** The commonly used name of our children's service. The Approved Provider is Pre-School Association Middle Park Incorporated on our license (PSAMPI).

**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 not limited to Dropbox, Google Drive, One Drive, WhatsApp.

**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.

**Personal Electronic Device:** A device that can take photos or record videos refers to any handheld or portable device owned by an individual, such as a smartphone, tablet, or digital camera, 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.

**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, SMS, Facebook Messenger, TikTok and Instagram

**Spam:** Unsolicited and unwanted emails or other electronic communication.

**KITP:** The Kindergarten Information Technology Program delivered by the State Library Victoria providing information technology support to kindergarten's, free of charge.

**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

- Acceptable Use Policy, DE 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](http://www.kindergarten.vic.gov.au)
- National Model Code - Taking images in early childhood education and care: <https://www.acecqa.gov.au/national-model-code-taking-images-early-childhood-education-and-care>
  - Full Code link here....<https://www.acecqa.gov.au/sites/default/files/2024-07/National%20Model%20Code%20Taking%20Images%20and%20Videos.pdf>
- Child Safe Environment and Wellbeing
- Code of Conduct Policy
- Compliments and Complaints
- Educational Program
- Enrolment and Orientation
- eSafety for Children
- Governance and Management of the Service
- 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)*)



## ATTACHMENTS

- Attachment 1: Procedures for use of ICT at the service
- Attachment 2: Unacceptable/inappropriate use of ICT facilities
- Attachment 3: Social Media Guidelines
- Attachment 4: Authorised user agreement
- Attachment 5: Parent/guardian authorisation for under-age access to the Civic Kindergarten ICT facilities:
- Attachment 6: Authorised Use of Personal Device Form
- Attachment 7: **National Model Code For Early Childhood Education And Care** - Taking Images or Videos of Children while providing Early Childhood Education and Care
- Attachment 8: Risk Assessment Online Environment

## AUTHORISATION



This policy was adopted by the approved provider of Civic Kindergarten on 15<sup>th</sup> August 2024.

**REVIEW DATE:** AUGUST 2025

## DOCUMENT HISTORY

Version	Date	By	Reason for change
1.0	2014	ELAA	ELAA template updated in 2015
2.0	August 2017	Policy Officer	Review and endorsement by Committee of Management (CoM)
3.0	November 2020	Policy Officer	Reviewed and endorsed by CoM.
4.0	March 2021	Policy Officer	Reviewed and endorsed by CoM.
5.0	August 2024	President, Director	Reviewed and endorsed by CoM.



## ATTACHMENT 1. PROCEDURES FOR USE OF ICT AT THE SERVICE

### Email usage

- Content of emails and email addresses must always be checked before sending.
- When sending emails to multiple recipients, care should be taken to avoid the inappropriate disclosure of email addresses to a whole group of recipients; blind copying (BCC) should be used where appropriate.
- Always include a subject description in the subject line.
- 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.
- Move unauthorised or identified junk emails to the 'junk' folder to ensure any future emails do not land in the inbox. Do not move these type of emails to the trash folder.
- Check email accounts on a regular basis and forward relevant emails to the approved provider or appropriate committee members/staff.
- Back up old correspondence to the hard drive quarterly.
- Respond to emails as soon as is practicable.
- Never send unauthorised marketing content or solicitation emails
- Be suspicious of phishing titles.

### Digital storage of personal and health information

- Digital records containing personal, sensitive and/or health information, or photographs 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 photographs 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*)

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.

- ICT 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 (Onedrive) and also stored on an external backup drive, and 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.

- Backup plan identifies:
  - All files, emails, images & videos are backed up.
  - Manual back up's are saved to an external hard drive.
  - Manual back up's are performed quarterly with the assistance of KITP.
  - The Director/Operations Manager are in charge of performing backups.
  - The Director/Operations Manager monitor the success of these backups
  - Manual back up's saved on an external hard drive are kept in the locked cupboard in the kindergarten office.

Services can choose to either between onsite or remote backup:

- Onsite Backup
  - copy data to a hard drive, manually, quarterly.

- Remote Backup- cloud based backup server
  - Onedrive contains all files, emails and photo's and video's which is password protected.

## 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; updated as required by each system.
- 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.
- store passwords electronically with a password protect access by Director/Operations Manager.
- 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 or staff members are working from home they must:

- complete the authorised user agreement form (*refer to Attachment 4*)
- conduct a workstation assessment; taking reasonable care in choosing a suitable work space, including ergonomics, lighting, thermal comfort, safety, and privacy
- ensure security and confidentiality of work space, 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 Confidentially 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 ICT FACILITIES

Users of the ICT facilities (and in particular, the internet, email and social media) provided by Civic Kindergarten must not:

- create or exchange messages that are offensive, harassing, obscene or threatening
- create, copy, transmit or retransmit chain emails (*refer to Definitions*), spam (*refer to Definitions*) or other unauthorised mass communication
- use the ICT facilities as a platform to gain unauthorised access to other systems
- carry out activities that are illegal, inappropriate or offensive to fellow employees or the public. Such activities include, but are not limited to, hate speech or material that ridicules/discriminates against others on the basis of race, nationality, creed, religion, ability/disability, gender or sexual orientation
- use the ICT facilities to access, download, create, store or distribute illegal, offensive, obscene or objectionable material (including pornography and sexually explicit material). It will not be a defence to claim that the recipient was a consenting adult
- use the ICT facilities to make any personal communication that could suggest that such communication was made in that person's official capacity as an employee or volunteer of Civic Kindergarten
- play games
- use the facilities to assist any election campaign or lobby any government organisation
- exchange any confidential or sensitive information held by Civic Kindergarten 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 ICT at the service for unlawful purposes may be liable to criminal or civil legal action. This could result in serious consequences, such as a fine, damages and/or costs being awarded against the individual, or imprisonment. The Approved Provider will not defend or support any individual using the service's ICT facilities for an unlawful purpose.
- The service may block access to internet sites where inappropriate use is identified.
- Employees who fail to adhere to this policy may be liable to counselling, disciplinary action or dismissal.
- Management, educators, staff, volunteers and students who fail to adhere to this policy may have their access to the service's ICT facilities restricted/denied.

### 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 below directives are essential to the safety and wellbeing of staff, children and their families, and to ensure that Civic Kindergarten operates in a professional and appropriate manner when using social media and/or information sharing platforms.

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

It is a breach of confidentiality and privacy to make posts or comments about children, families, staff or management from Civic Kindergarten 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.

Civic Kindergarten specifically requires that, unless you have the express permission, you:

- Do not video or photograph anyone, or post photos or personal details of other Civic Kindergarten staff, children or families;
- Do not post photos or videos of Civic Kindergarten 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 Civic Kindergarten branded Facebook page, or other pages or content on social media that represents Civic Kindergarten, it's staff, children or families without authorisation from the approved provider;
- Do not post anything that could embarrass or damage the reputation of Civic Kindergarten, 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 Civic Kindergarten reputation or bring it into disrepute;
- imply that they are authorised to speak as a representative of Civic Kindergarten, or give the impression that the views expressed are those of Civic Kindergarten, unless authorised to do so
- use a Civic Kindergarten email address or any Civic Kindergarten 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 Civic Kindergarten;
- use or disclose any confidential information or personal information obtained in the capacity as an employee/contractor of Civic Kindergarten; or
- access and/or post on personal social media during paid workhours.

### Parents/Guardians must to note:

- Civic Kindergarten will provide parents/guardians with exclusive access (two maximum access accounts per child) to access their child's kindergarten portfolio via use of the password protected, closed circuit Storypark application to review their child's progress/activity captured at kindergarten.
- Parents/Guardians are not to share their passwords to Storypark.
- Parents/Guardians are to be advised use of WhatsApp Group or SMS Groups for the purpose of communicating with other parents/guardians at the service are entirely independent from Civic Kindergarten. Civic Kindergarten and staff do not govern or manage those platforms nor its use.

### Personal use of social media

Civic Kindergarten 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 Civic Kindergarten that can occur through their use of social media, even if their activity takes place outside working hours or on devices not owned by Civic Kindergarten.

If an individual can be identified as an employee of Civic Kindergarten 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 Civic Kindergarten
- expressly state on all postings (identifying them as an employee of Civic Kindergarten) the stated views are their own and are not those of Civic Kindergarten;
- 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 Civic Kindergarten 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**

- Civic Kindergarten 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 Civic Kindergarten *Code of Conduct Policy*.
- Civic Kindergarten may request that any information contained on any social media platform that is in breach of this policy be deleted.
- Civic Kindergarten may restrict an employee's access to social media on [Civic Kindergarten ICT facilities or if they are found to have breached this policy or while Civic Kindergarten 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 Civic Kindergarten
- will ensure that the PSD:
  - is used for work-related purposes only
  - is password-protected at all times
  - will not be loaned to unauthorised persons
  - will be returned to Civic Kindergarten on cessation of employment
- will notify the Civic Kindergarten President as soon as is practicable if the PSD is damaged, faulty or lost
- have read the Civic Kindergarten Information and Communication (ICT) Technology 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 CIVIC KINDERGARTEN ICT FACILITIES

Student's name: \_\_\_\_\_

Date of placement: \_\_\_\_\_

I, \_\_\_\_\_, am a parent/guardian of

\_\_\_\_\_

I have read the Civic Kindergarten *Information and Communication Technology (ICT) Policy* and agree to the conditions of use of the service's ICT facilities for the above-named student.

I also understand that Civic Kindergarten provides no censorship of access to ICT facilities.

\_\_\_\_\_  
Signature (student)

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature (parent/guardian)

\_\_\_\_\_  
Date



## ATTACHMENT 6: AUTHORISED USE OF PERSONAL DEVICE FORM

### Section 1: Personal Details

Staff Member Name:

Position:

Personal Device Type (e.g., Smartphone, Tablet):

Date of use:

### Section 2: Purpose

This form grants permission for the above-named staff member to use their personal device to take photos or videos of children for educational and documentation purposes at Civic Kindergarten if the service does not have enough or working devices.

### Section 3: Guidelines

#### 1. Consent:

- Photos and videos of children can only be taken if explicit written consent has been obtained from the parents/guardians or guardians of each child.

#### 2. Usage:

- Personal devices may not be used for taking photos or videos and must be put away when not in use.
- Photos and videos must be used solely for the purposes outlined in the consent forms (e.g., educational documentation, sharing with parents/guardians/guardians).

#### 3. Privacy and Security:

- Photos and videos must be stored securely and must not be shared on any personal social media accounts or with unauthorised individuals.
- Devices must be password-protected and encrypted to ensure the safety of the content.

#### 4. Deletion and Retention:

- Photos and videos must be transferred to Civic Kindergarten secure storage within 24 hours and deleted from the personal device immediately after transfer.
- Photos and videos must be retained and disposed of in accordance with Civic Kindergarten *Information Technology and Communication Policy*

#### 5. Professional Conduct:

- Staff must maintain a professional demeanour while using personal devices.
- Authorised use of personal device forms 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:

Approved Provide/Nominated Supervisor Name:

Approved Provide/Nominated Supervisor Signature:

Date

# ATTACHMENT 7: NATIONAL MODEL CODE FOR EARLY CHILDHOOD EDUCATION AND CARE

## Taking Images or Videos of Children while providing Early Childhood Education and Care

ACECQA, in partnership with all governments, has released a set of recommended child safe practices for using electronic devices, when taking images or videos of children in early childhood education and care (ECEC).

**Guidelines link:** <https://www.acecqa.gov.au/sites/default/files/2024-07/Guidelines%20for%20the%20National%20Model%20Code%20Taking%20Images%20and%20Videos.pdf>

**Frequently Asked Question links:** <https://www.acecqa.gov.au/sites/default/files/2024-07/National%20Model%20Code%20FAQS%20-%20Final.pdf>

### NATIONAL MODEL CODE FOR EARLY CHILDHOOD EDUCATION AND CARE



#### TAKING IMAGES OR VIDEOS OF CHILDREN WHILE PROVIDING EARLY CHILDHOOD EDUCATION AND CARE



##### Purpose

The National Model Code for Taking Images or Videos of Children while Providing Early Childhood Education and Care (National Model Code) addresses child safe practices for the use of electronic devices while providing early childhood education and care (ECEC). Providers of centre-based ECEC under the National Quality Framework (NQF) are strongly encouraged to adopt the National Model Code as a further support to promote a child safe culture. The National Model Code is a voluntary, interim measure while future legislative reform is being considered by governments.



##### Scope

This National Model Code has been developed for approved providers and their services, including educators, other staff, and volunteers, while children are being educated and cared for at centre-based early childhood services. While the National Model Code targets centre-based services whose primary purpose is to educate and care for children 0-5 years old under the NQF (long day care and pre-school / kindergarten services), providers of other types of children's education and care services may wish to consider adopting similar practices within their own contexts.

##### National Model Code

###### Part 1

Only service-issued electronic devices should be used when taking images or videos of children while providing education and care. The appropriate use of service-issued electronic devices for taking, sending and storing images or videos of children should be clearly outlined in policies and procedures.

###### Part 2

Personal electronic devices that can take images or videos (such as tablets, phones, digital cameras, and smart watches) and personal storage and file transfer media (such as SD cards, USB drives, hard drives and cloud storage) should not be in the possession of any person while providing education and care and working directly with children. Any exceptions to this should be for limited, essential purposes that are authorised in writing (or through another means if written authorisation is not reasonably practicable) by the approved provider of the service, and where that access does not impede the active supervision of children.

###### Part 3

Essential purposes for which 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 a 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.

###### Part 4

Approved providers and their services should have strict controls in place for the appropriate storage and retention of images and videos of children.

##### Guidelines

Guidelines have been developed to support approved providers and their services apply the National Model Code in their context(s) and uphold child safe practices when using electronic devices to take images or videos of children.

## ATTACHMENT 8: RISK ASSESSMENT ONLINE ENVIRONMENT

<b>Date reviewed</b>	August 2024
<b>Next review due</b>	August 2025
<b>Activity</b>	Online Environment

Types of risk	Types of harm	Existing risk controls	Risk Assessment	New controls required
<b>Situational risk: Photo, Image and Video's of Children in care.</b>				
Privacy and Security Risk.	<p>Unauthorised access to or misuse of children's images and videos.</p> <p>Exposure of children to individuals not authorised to view their media.</p>	<p>Code of Conduct with employees and enrolled children's parents/guardians/guardians.</p> <p>National Model Code for Early Childhood Education and Care.</p> <p>Images &amp; video's currently only recorded on dedicated kindergarten SLR camera. Images downloaded manually onto office computer and uploaded to Storypark in line with the parent/guardian's permission provided prior to enrolment.</p> <p>Strict access controls on the Storypark (closed circuit) platform to ensure only authorised individuals (staff and parents/guardians) can view photos and videos respectively.</p> <p>Obtaining explicit parental consent for the collection, use, and sharing of children's media.</p>	High	<p>Clear guidelines and consent forms for media usage, including opt-out options for parents/guardians.</p> <p>Encryption of media files to protect against Unauthorised access via Storypark.</p> <p>Publicly display National Model Code policy posters for handling and sharing images, video's including guidelines for consent and usage, display poster in the foyer and website.</p> <p>Code of Conduct and Child Safety and Wellbeing Policy include specific content about behaviour online/by phone. Share with children, young people and parents/guardians/carers.</p> <p>Tell children, young people and parents/guardians/carers what sort of communication they can expect from staff online/by phone, so they know if contact from staff is not authorised.</p> <p>Hold a staff meetings to discuss the Code of Conduct including appropriate behaviour online/by phone.</p> <p>Share resources with parents/guardians/guardians about online bullying from the eSafety Commissioner and tell them how they can raise concerns.</p>

Types of risk	Types of harm	Existing risk controls	Risk Assessment	New controls required
Situational risk: Data Breaches				
Cybersecurity and Privacy Risk	<p>Exposure of personal information could lead to privacy violations and identity theft.</p> <p>Damage to the kindergarten's reputation and trust among parents/guardians.</p>	<p>Storypark employs strong encryption and security protocols.</p> <p>Regularly update passwords and ensure they are strong.</p> <p>Educate staff about data protection policies and ensure compliance.</p>	High	<p>Regular security audits.</p> <p>Multi-factor authentication (MFA) for accessing sensitive data.</p> <p>Data breach response plan, including notification procedures.</p>
Situational risk: Hacking				
Cybersecurity Risk	<p>Unauthorised access to the closed circuit platform Storypark, potentially leading to data compromise and service disruption.</p> <p>Theft or manipulation of sensitive data.</p> <p>Enrolment Application emails containing viruses within the attachments.</p>	<p>Storypark platform provides infrastructure with industry-standard encryption and firewalls.</p> <p>Storypark complete regular updates and patching to address vulnerabilities.</p> <p>IT Support (State Library Victoria Free Kindergarten IT Program) provides infrastructure with encryption and firewalls</p>	High	<p>Continuous monitoring for suspicious activities and potential threats.</p> <p>Staff and parent/guardian education on recognising phishing attacks and other cyber threats.</p> <p>Regular updates to the platform's security measures and incident response protocols.</p>
Situational risk: Storage of Files				
Data Security Risk	<p>Loss or Unauthorised access to important documents and records.</p> <p>Risk of data breaches or data corruption.</p>	<p>Secure cloud storage solutions with encrypted data storage.</p> <p>Access controls to limit file access to authorised users only.</p>	Medium	<p>Implement regular backup procedures to ensure data recovery in case of loss or corruption.</p> <p>Review and update access permissions regularly to ensure appropriate levels of access.</p> <p>Encrypt files before storing them, especially sensitive documents.</p>

Types of risk	Types of harm	Existing risk controls	Risk Assessment	New controls required
Situational risk: Parents/guardians Sharing Passwords				
Account Security Risk	<p>Unauthorised access to the platform, leading to potential data breaches or misuse of the account.</p> <p>Compromise of personal and sensitive information.</p>	<p>Strong password policies requiring complex and unique passwords.</p> <p>Guidelines advising against sharing passwords among parents/guardians and staff.</p>	Medium	<p>Regular reminders and educational sessions for parents/guardians/guardians on the importance of password security.</p> <p>Providing parents/guardians/guardians the option to implement single sign-on (SSO) solutions or multi-factor authentication (MFA) to enhance security via Storypark.</p>
Situational risk: Inappropriate Content Sharing				
Content Management Risk	<p>Exposure to inappropriate or harmful content.</p> <p>Breach of privacy and trust.</p>	<p>Content moderation policies and controls in place to monitor and manage shared content.</p> <p>Guidelines for acceptable use and sharing of content on the platform.</p>	Medium	<p>Communicate information for staff and parents/guardians/guardians on acceptable content and behaviour.</p> <p>Implement automated content filtering tools where possible to detect and prevent inappropriate content.</p> <p>Regularly review content shared on the platform to ensure compliance with policies.</p>
Situational risk: Legal and Compliance Issues				
Regulatory Compliance Risk	<p>Legal penalties for non-compliance with data protection laws.</p> <p>Damage to the kindergarten's reputation and operational impact.</p>	<p>Compliance with privacy laws and regulations (e.g., Privacy Act 1988).</p> <p>Regular legal consultations to ensure adherence to data protection requirements.</p>	Medium	<p>Regular updates to privacy policies and procedures in line with new or amended regulations.</p> <p>Train staff on legal and compliance aspects related to data protection and privacy.</p> <p>Conduct periodic compliance audits to ensure adherence to relevant laws.</p>