INFORMATION & COMMUNICATION TECHNOLOGY

QUALITY AREA 7 |

PURPOSE

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

- understand and follow procedures to ensure the safe and appropriate use of ICT at an ECKA service, 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

an ECKA service is committed to:

- professional, ethical and responsible use of ICT at ECKA services
- 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 and 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 an ECKA service. **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 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
- viewing material electronically
- weblogs (blogs)
- private online service for sharing information with families e.g. Storypark

RESPONSIBILITIES	Approved provider and persons with management or control	Nominated supervisor and persons in day-to-day charge	Early childhood teacher, educators and all other staff	Parents/guardians	Contractors, volunteers and students
R indicates legislation requirement, and should not be deleted					
Ensuring that the use of the service's ICT complies with all relevant state and federal legislation *(refer to Legislation and standards),* and all service policies *(including Privacy and Confidentiality Policy and Code of Conduct Policy)*	**R**	√	√	√	√
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 (*refer to Definitions)* while educating and care for children *(refer to Attachment 6)*	√	√			
Ensuirng that staff don't not carry their personal electronic devices *(refer to Definitions)* while providing education and care to children, except for authorised essential purposes	√	√	√		√
Managing inappropriate use of ICT as described in *Attachment 2*	**R**	√			
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 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 *(refer to Attachment 1)*	√	√			
Embedding a culture of awareness and understanding of security issues at the service	**R**	√	√	√	√
Ensuring that ECKA devices are not connected to any unsecured or public Wi-fi for example cafés, motels, events and if internet connection is required to use mobile phone hotspot instead.	√	√	√	√	√
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	**R**	√			
Ensuring that the service's computer software and hardware are purchased from an appropriate and reputable supplier	√	√			
Ensure that when members of the public have access to the service that all portable devices e.g. laptops, phones, iPads are securely stored to prevent theft	√	√	√		
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 *(refer to Attachment 1)*	√	√	√		
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**	√	√		
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**		
Use extreme caution when opening email attachments received from unknown senders: these may contain viruses, malware or Trojan horse code.	√	√	√	√	√
Ensure that unauthorised software is not downloaded or unauthorised devices e.g USBs, scanners, digital cameras are attached to computers without authorisation from ECKA management.	√	√	√	√	√
Considering encryption *(refer to Definitions)* of data for extra security	√	√			
Ensuring that reputable anti-virus and firewall software *(refer to Definitions)* are installed on service computers, and that software is kept up to date	√	√			
Developing procedures to minimise unauthorised access, use and disclosure of information and data, which may include	**R**	√			

limiting access and passwords, and encryption *(refer to Definitions)*					
Ensuring that the service's liability in the event of security breaches, or unauthorised access, use and disclosure of information and data is limited by developing and publishing appropriate disclaimers *(refer to Definitions)*	**R**	√			
Report immediately to ECKA's Operations Manager if management, early childhood teachers, educators, staff or others at the service believe the computer system has been subject to a security breach or unauthorised access.	√	√	√		√
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 *(refer to Definitions)* by ICT users at the service	**R**	√	√	√	√
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**	√	√		√
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**	√			√
Providing authorisation to early childhood teachers, educators and staff to be social media representatives for an ECKA service *(refer to Attachment 3)*	√	√			
Complying with all relevant legislation and service policies, protocols and procedures, including those outlined in *Attachments 1*	√	√	√	√	√
Reading and understanding what constitutes inappropriate use of ICT *(refer to Attachment 2)*	√	√	√	√	√
Completing the authorised user agreement form *(refer to Attachment 4)*	√	√	√		√
Maintaining the security of ICT facilities belonging to an ECKA service 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		√	√		√
Co-operating with other users of the service's ICT to ensure fair and equitable access to resources	√	√	√		√
Obtaining approval from the approved provider before purchasing licensed computer software and hardware		√	√		
Ensuring no illegal material is transmitted at any time via any ICT medium *(refer to Attachment 2)*	**R**	√	√	√	√

Using the service's email, messaging and social media *(refer to Definitions)* facilities for service-related and lawful activities only *(refer to Attachment 2)*	√	√	√	√	√
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		√	√		√
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) *(refer to Attachment 4)*		√	√		√
Restricting the use of personal mobile phones or other smart devices that are able to capture or store images -such as smart watches, to rostered breaks, and only used in areas outside of spaces being utilised for education and care of children	√	√	√	√	√
Responding only to emergency phone calls when responsible for supervising children to ensure adequate supervision of children at all times *(refer to Supervision of Children Policy)*	√	√	√		√
Ensuring electronic files containing information about children and families are kept secure at all times *(refer to Privacy and Confidentiality Policy)*	**R**	**R**	**R**		**R**
Responding to a privacy breach in accordance with *Privacy and Confidentiality policy.*	**R**	√			
Complying with the appropriate use of social media *(refer to Definitions)* platforms *(refer to Attachment 3)*	√	√	√		√
Complying with this policy at all times to protect the privacy, confidentiality and interests of an ECKA service 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 organization 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

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
Commonwealth Legislation – Federal Register of Legislation: 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.

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: include but not limited to the necessity for maintaining physical health, availability for emergency contact by dependants where an alternative method of contact is not available.

Firewall: The primary method of keeping a computer/network secure. A firewall controls (by permitting or restricting) traffic into and out of a computer/network and, as a result, can protect these from damage by unauthorised users.

Flash drive: A small data-storage device that uses flash memory, and has a built-in USB connection. Flash drives have many names, including jump drives, thumb drives, pen drives and USB keychain drives.

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

Integrity: (In relation to this policy) refers to the accuracy of data. Loss of data integrity may be either gross and evident (e.g. a computer disk failing) or subtle (e.g. the alteration of information in an electronic file).

Malware: Short for 'malicious software'. Malware is intended to damage or disable computers or computer systems.

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, 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

- Acceptable Use Policy, DE Information, Communications and Technology (ICT) Resources: https://www.education.vic.gov.au/school/teachers/management/infrastructure/Pages/acceptableuse.aspx
- ELAA Information and Communication Policy
- IT for Kindergartens: 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

RELATED POLICIES

- Child Safe Environment and Wellbeing
- Code of Conduct
- 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: AI Guidelines
- Attachment 5: Authorised user agreement

- Attachment 6: Parent/guardian authorisation for under-age access to the an ECKA service ICT facilities:
- Attachment 7: Authorised Use of Personal Device Form

AUTHORISATION

This policy was adopted by the approved provider of an ECKA service on 16/10/2012.

This Policy was last reviewed: 30/8/2023, 5/8/2024

REVIEW DATE: 30/06/2026

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.
- 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.

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)*
  - 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.
- 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 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
  - Where it's being backed up
  - How often backups will occur
  - Who's in charge of performing backups
  - Who's in charge of monitoring the success of these backups
  - How will backup drives be stored securely
- Services must use onsite backup – ***do not use remote cloud based backup***. Turn off cloud back-up automatic options. Seek advice from the ECKA office if unsure whether your devices are backing up to the cloud.

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 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, heath 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 Confidently Policy*

ensure that any wifi access is secure

report breaches to privacy or loss of private, sensitive, and heath 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 an ECKA service 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 an ECKA service
- 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 an ECKA service 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 an ECKA service 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 an ECKA service.

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

ECKA specifically requires that, unless you have the express permission, you:

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

Personal use of social media

an ECKA service 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 an ECKA service or individual ECKA Service that can occur through their use of social media, even if their activity takes place outside working hours or on devices not owned by an ECKA service.

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

an ECKA service 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 an ECKA service *Code of Conduct Policy*.

an ECKA service may request that any information contained on any social media platform that is in breach of this policy be deleted.

an ECKA service may restrict an employee's access to social media on [an ECKA service ICT facilities or if they are found to have breached this policy or while an ECKA service investigates whether they have breached this policy.

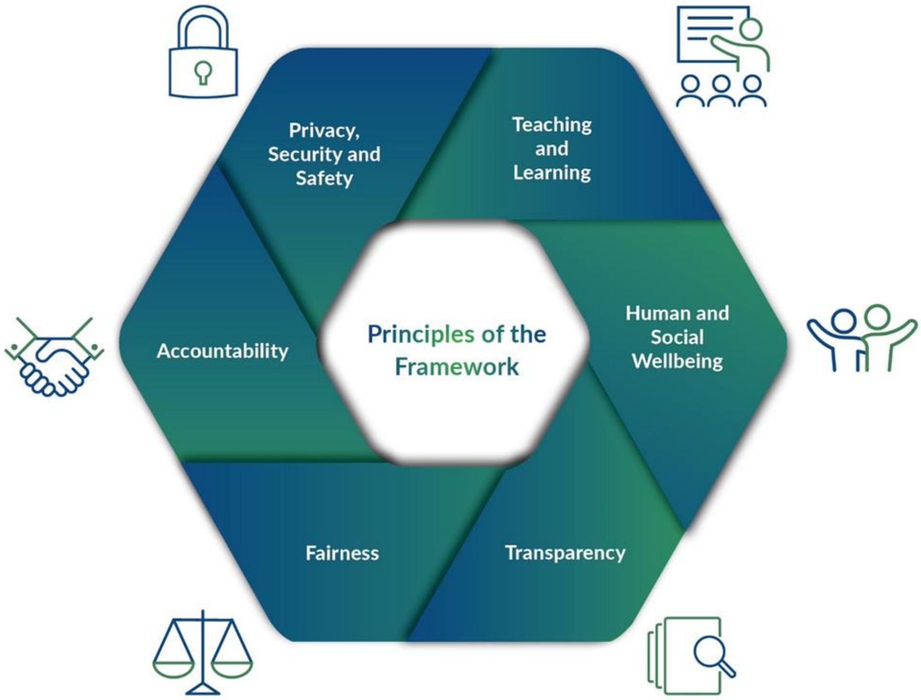
ATTACHMENT 5. AI GUIDELINES

This guide sets out requirements for ECKA employees that choose to explore the use of generative artificial intelligence (AI) tools. It provides advice around how to use generative AI tools in a safe and responsible way.

Details

On 1 December 2023, Education ministers released the Australian Framework for Generative Artificial Intelligence in Schools (the National Framework). The aim of the National Framework is to provide guidance on understanding, using and responding to generative AI. It includes 6 principles and 25 guiding statements that define what safe, ethical, and responsible use of generative AI should look like in Australian schools. This policy, guidance and resources are designed to complement the National Framework.

https://www.education.gov.au/schooling/announcements/australian-framework-generative-artificial-intelligence-ai-schools


Privacy, Security and Safety
Teaching and Learning
Principles of the Framework
Accountability
Human and Social Wellbeing
Fairness
Transparency

ECKA employees must comply with the requirements detailed in this guide when using generative AI in all contexts.

- ECKA employees may use generative AI tools if use;
  - complies with the requirements of this guide
  - protects privacy and personal data
  - complies with appropriate use of generative AI tools
  - complies with other relevant policies that are not specific to generative AI, such as ECKA' Communication and IT Policy, Privacy and Confidentiality Policy and is accompanied by reasonable steps to identify, understand and appropriately manage risks.

Prior to implementation of any generative AI tool, ECKA employees should:

- clearly define expected benefits and risks in using AI tools,
- Protect privacy and personal data

ECKA employees are expected to take reasonable steps to ensure the protection of data entered into generative AI tools or software that integrates generative AI tools (including user prompts). They should do this by prioritising the use of tools that:

- do not share this data with third parties
- do not use this data to train a generative AI model

- do not save or store data for future use by the provider of the tool.
- not load any personal information about children, families or employees into the tool (for example, names, reports, personal histories and contact details).
- not enter any information about ECKA or any of its Services that is sensitive and can be identified as being ECKA or the Kindergarten. This is because content may be used and reused by the platform and its users, which may constitute a privacy breach.

Appropriate use of generative AI tools

Where ECKA employees choose to use generative AI tools, they are directed to:

- not upload media including ECKA and Kindergarten logos, depictions of children, staff, or parents (for example, photos, audio, video), or generate images or other media in the likeness of these persons.
- not generate artefacts that mimic a cultural tradition in a way that is disrespectful or offensive (for example, images mimicking Koorie artwork).
- not use generative AI tools to communicate with parents in ways that undermine authentic relationships or replace the unique voice and professional judgement of teachers and educators This includes not using generative AI tools to directly:
  - communicate with parents
  - make judgements about children's learning and development, or progress
  - write reports about children for parents or carers.
  - review the information generated by AI to ensure that the content accurately reflects the information required and is written in the correct context.

During implementation of any generative AI tool, ECKA employees should:

- ensure the use of generative AI tools is disclosed when tools have an impact on others.
- ensure monitoring of benefits and risks
- consider de-implementing any tool if benefits are not realised or risks are not being adequately managed.

Related policies

- Child Safe Environment and Wellbeing Policy
- Code of Conduct
- eSafety for Children
- Inclusion and Equity
- Information Communication Technologies
- Interactions with Children
- Participation of Volunteers and Students
- Privacy and Confidentiality

Definitions

Generative artificial intelligence (AI)

Generative AI is a type of computer-based model that can generate new content or modify existing content in response to user prompts. The inputs and outputs of generative AI tools can include text, images, audio, computer code, and other types of data. Refer to the Guidance tab for more information about generative AI.

Personal information

Personal information is recorded information or opinion, whether true or not, about a person whose identity is apparent, or can reasonably be ascertained, from the information. The information or opinion can be recorded in any form. A person's name, address, phone number and date of birth (age) are all examples of personal information.

Department of Education Guidance:

What is generative AI?

Generative artificial intelligence (AI) is a type of computer-based model that can generate new content or modify existing content in response to user prompts. The inputs and outputs of generative AI tools can include text, images, audio, computer code, and other types of data. Generative AI tools use machine learning, a process where tools are trained to recognise complex patterns in large datasets. This enables them to produce outputs that can closely resemble human-generated content without explicit programming.

Common types of generative AI tools and functions

Common types of generative AI tools and functions are outlined below, noting that the examples are provided for illustrative purposes only and are not specifically recommended or endorsed. Generative AI tools and functions can be provided through standalone products or embedded into other software and applications. Some generative AI tools combine multiple functions into one product.

- Text generation – specialising in producing human-like text (tools that do this are sometimes known as large language models (LLMs)
- Image generation – able to transform text into images or create images
- Video generation – able to create videos or edit existing videos
- Audio generation – able to create audio files, such as music, speech, or sound effects
- Code generation – can produce computer programming code, such as Python, Java, or C++
- Design generation – can produce layouts, visual compositions, and graphical elements for a wide range of design projects

PROTECTING PRIVACY AND PERSONAL DATA

Privacy and data risks:

Generative artificial intelligence (AI) tools pose unique privacy and data protection risks that are important to be aware of. For example:

- generative AI providers may request or require data that includes personal, sensitive or health information to provide access to their generative AI tools
- some generative AI tools have the capacity to match data inputs with other information about individuals, which increases privacy risk through building individual data profiles
- the safety and storage processes of data inputs into generative AI tools may be unclear
- it may be difficult or impossible for a generative AI model to forget personal, sensitive or health information once it has been uploaded
- inputs copied from the internet or from untrustworthy sources, when pasted as a prompt into a generative AI tool, may cause the tool to behave in unexpected or unsafe ways (for example, an image copied from the internet and pasted into a multimodal generative AI tool, may have invisible text embedded within it that the user was not aware of). This is sometimes referred to as a 'prompt injection'
- content generated by generative AI about a person can constitute a new collection of personal information about that individual, which can be seen as unreasonably intrusive and therefore a breach of privacy.

ATTACHMENT 5. AUTHORISED USER AGREEMENT

Portable storage device (PSD) (including laptops)

I, ____ ,

acknowledge that I have received a PSD belonging to an ECKA service
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 an ECKA service on cessation of employment

will notify the Operations Manager as soon as is practicable if the PSD is damaged, faulty or lost
have read the an ECKA service 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 6. PARENT/GUARDIAN AUTHORISATION FOR UNDER-AGE ACCESS TO THE [……………………………………SERVICE NAME] ICT FACILITIES

Student's name: ____

Date of placement: ____

I, ____________________________________ , am a parent/guardian of

____

I have read the an ECKA service *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 an ECKA service provides no censorship of access to ICT facilities.

______________________________	______________________________
Signature (student)	Date
______________________________	______________________________
Signature (parent/guardian)	Date

ATTACHMENT 7: AUTHORISED USE OF PERSONAL DEVICE FORM

Section 1: Personal Details

Staff Member Name: Position:

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

Date/s of use:

Reason for use of personal device while working with children:

Section 2: Purpose

This form grants permission for the above-named staff member to have their personal device for the reason/s and date/stated above while working with children an ECKA service

Section 3: Guidelines

Usage:

- Personal devices may only be used for the purpose/s stated above during scheduled activities and must be put away when not in use.
- Personal devices must not be used to capture or store images of children

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.
- Access to personal device for the purpose/s stated above must not prevent the staff member from fulfilling all responsibilities including supervision and engagement with children.

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 Provider/Nominated Supervisor Name:

Approved Provide/Nominated Supervisor Signature: | Date