

ONLINE SAFETY Policy

# PURPOSE

This policy will provide guidelines to ensure that all use of digital, electronic or online platforms (referred to collectively as online platforms) by or involving children at, on behalf of, or in collaboration with Elonera Pre School:

* Is safe and appropriate at all times.
* Prioritises the privacy, confidentiality and safety of the children at all times.
* Complies with all relevant legislation, regulation and the standards and policies of the Service.

# Policy statement

## Values

Elonera Pre Schoolis committed to:

* the safe, professional, ethical and responsible use of online platforms by or involving the children at theservice, including that all use shall be:
	+ age and developmentally appropriate;
	+ for the benefit of child’s learning and social development;
	+ an extension of the educational program;
	+ focused on small group interaction rather than children working in isolation; and
	+ followed by other learning opportunities and experiences.
* providing a safe space for management, educators, staff, children and others using the service’s facilities for the purposes of online learning and communication.
* assessing and understanding the risks associated with online learning for children, families, educators and the service more generally.
* safeguarding the privacy and confidentiality of information received, transmitted or stored electronically and ensuring the privacy of the children is paramount at all times.
* ensuring that the use of the service’s facilities by the children for the purposes of online learning or communication 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 and the safe and responsible use of online platforms by or involving children at the service.

## Scope

This policy applies to the Approved Provider, Persons with Management and Control, Nominated Supervisor, Persons in Day to Day Charge, educators, staff, students on placement, volunteers and children at Elonera Pre School. This policy relates to the use of online platforms via information communication technology (ICT) facilities at Elonera Pre School by or with children as an extension of the education program. For information relating to use of information communication technology (ICT) generally, you should refer to the *Information Communication and Technology Policy*.

This policy applies to all aspects of the use of online platforms by or with the children, including but not limited to:

* internet usage
* electronic discussion groups
* social networking
* file transfer
* file sharing
* video conferencing
* streaming media
* instant messaging
* online discussion groups and chat facilities
* copying, saving or distributing files
* viewing material electronically
* printing material

## Background and legislation

#### Background

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.

The National Principles for Child Safe Organisations recognise the importance of safe physical and online environments to promote the safety and wellbeing of all children. Early learning services have responsibility to ensure children and educators are protected from harm when they engage with digital platforms.

State and federal laws, including those governing child safety, information privacy, copyright, anti-discrimination and sexual harassment, apply to the use of online platforms (refer to *Legislation and standards*). Illegal and inappropriate use of online platforms includes pornography, cyber bullying, defamation, breach of copyright, unlawful discrimination or vilification, harassment (including sexual harassment, stalking and privacy violations) and illegal activity, including illegal peer-to-peer file sharing.

#### Legislation and standards

Relevant legislation and standards include but are not limited to:

* *Charter of Human Rights and Responsibilities Act 2006* (Vic)
* *Children, Youth and Families Act 2005* (Vic)
* *Child Safety and Wellbeing Act 2005* (Vic)
* *Child Safe Standards* (Vic)
* *Crimes Amendment (Protection of Children) Act 2014* (Vic)
* *Classification (Publications, Films and Computer Games) Act 1995*
* *Commonwealth Classification (Publication, Films and Computer Games) Act 1995*
* *Copyright Act 1968* (Cth)
* *Copyright Amendment Act 2006* (Cth)
* *Education and Care Services National Law Act 2010*
* *Education and Care Services National Regulations 2011*
* *Equal Opportunity Act 2010* (Vic)
* *Family Law Act 1975* (Cth)
* *Freedom of Information Act 1982*
* *Health Records Act 2001* (Vic)
* *Information Privacy Act 2000* (Vic)
* *National Principles for Child Safe Organisations*
* *National Quality Standard*, Quality Area 2: Children’s health and safety
* *Privacy Act 1988* (Cth)
* *Privacy and Data Protection Act 2014 (Vic)*
* *Public Records Act 1973* (Vic)
* *Reportable Conduct Scheme* administered by the Commission for Children and Young People (Vic)
* *Working with Children Act 2005* (Vic)
* *Working with Children Regulations* (Vic)
* *Wrongs Act 1958* (Vic)
* *Sex Discrimination Act 1984* (Cth)
* *Trade Marks Act 1995* (Cth)



## Definitions

The terms defined in this section relate specifically to this policy. For commonly used terms e.g. Approved Provider, Nominated Supervisor, Regulatory Authority etc. refer to the *General Definitions* section of the current PolicyWorks Manual.

**Chain email:** An email instructing recipients to send out multiple copies of the same email so that circulation increases exponentially.

**Defamation:** To injure or harm another person’s reputation without good reason or justification. Defamation is often in the form of slander or libel.

**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.

**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).

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

**Security:** (In relation to this policy) refers to the protection of data against unauthorised access, ensuring confidentiality of information, integrity of data and the appropriate use of computer systems and other resources.

**Virus:** A program or programming code that multiplies by being copied to another program, computer or document. Viruses can be sent in attachments to an email or file, or be present on a disk or CD. While some viruses are benign or playful in intent, others can be quite harmful: erasing data or requiring the reformatting of hard drives.

## Sources and related policies

#### Sources

* *Early Years: Online Safety for Under 5s*, Australian Government eSafety Commissioner, https://www.esafety.gov.au/educators/esafety-early-years-program-for-educators
* *National Principles for Child Safe Organisations*, Child Safe Organisations, https://childsafe.humanrights.gov.au/sites/default/files/2019-02/National\_Principles\_for\_Child\_Safe\_Organisations2019.pdf
* *Statement on Young Children and Digital Technologies*, Early Childhood Australia, http://www.earlychildhoodaustralia.org.au/wp-content/uploads/2018/10/Digital-policy-statement.pdf" http://www.earlychildhoodaustralia.org.au/wp-content/uploads/2018/10/Digital-policy-statement.pdf

#### Service policies

* *Child Safe Environment Policy*
* *Code of Conduct Policy*
* *Complaints and Grievances Policy*
* *Curriculum Development Policy*
* *Governance and Management of the Service Policy*
* *Information Communication Technology Policy*
* *Interactions with Children Policy*
* *Privacy and Confidentiality Policy*
* *Supervision of Children Policy*

# Procedures

#### The Approved Provider or Persons with Management and Control is responsible for:

* ensuring that the use of online platforms by children attending the service complies with all relevant state and federal legislation (refer to *Legislation and standards*), and all service policies (including *Privacy and Confidentiality Policy*, *Code of Conduct Policy and Child Safe Environment Policy*)
* providing leadership for an organisational culture of appropriate use of online platforms and eSafety which is open to scrutiny and is continuously reviewed and improved
* providing suitable ICT facilities to enable educators and staff to effectively manage and operate the delivery of digital or online experiences by the children as part of the education program
* authorising the access of educators, staff, volunteers, students and children to the service’s ICT facilities, as appropriate
* providing clear procedures and protocols that outline the parameters for use of online platforms with children (refer to Attachment 1 – Procedures for use of online platforms with children at the service)
* embedding a culture of awareness and understanding of the risks associated with the use of online platforms (refer to Attachment 2 – eSafety checklist for early learning services)
* identifying the training needs of educators and staff in relation to eSafety, and providing recommendations for the inclusion of training in eSafety in professional development activities
* adhering to the requirements of the *Privacy and Confidentiality Policy* in relation to accessing and sharing information online
* developing procedures to ensure data and information (e.g. children’s names and images) are kept secure, and only disclosed to individuals where necessary e.g. to new educators, staff or committee of management
* developing procedures to ensure that all educators, staff, volunteers and students are aware of the requirements of this policy
* ensuring compliance with this policy and the Information Communication Technology Policy by all users of the service’s ICT facilities
* ensuring online platforms for use by children attending the service are age appropriate, educational, safe and secure, and (where practicable) have been endorsed or recommended by the Department of Education, eSafety Commissioner and/or other reputable organisations
* ensuring partner agencies participating in any online programs or initiatives with the children are appropriately screened and acknowledge and agree to comply with this policy and any related polices of the Service, including specifically the *Child Safe Environment Policy*.
* ensuring that written permission is provided by parents/guardians for authorised access to the service’s ICT facilities and any online platforms by children attending the service (refer to Attachment 3 – Parent/guardian authorisation for under-age access to online platforms via the use of Elonera Pre School ICT facilities).

#### The Nominated Supervisor, Person with Day to Day Charge, educators, staff and other authorised users of online platforms via the service’s ICT facilities are responsible for:

* complying with all relevant legislation and service policies, protocols and procedures, including those outlined above and in Attachment 1
* keeping allocated passwords secure, including not sharing passwords and logging off after using a computer
* allowing children to access accounts, data or files on Elonera ICT facilities only where authorisation has been provided
* co-operating with other users of online platforms endorsed by the service to ensure fair and equitable access to resources
* obtaining approval from the Approved Provider before using an online platform with children attending the service
* ensuring confidential and personal information is transmitted only on an as needs basis and with password protection or encryption, as practical
* ensuring no illegal material is transmitted at any time via any online platform
* using the service’s email, messaging and social media facilities for service-related and lawful activities only
* ensuring children using online platforms while at the service are doing so in a safe and open space and are supervised closely at all times
* ensuring when partner organisations are participating in the use of online platforms with children attending the service, that any participants have a Working With Children Check and that children participate only under strict supervision by an educator
* 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*)
* responding to a privacy breach in accordance with *Privacy and Confidentiality Policy*
* ensuring there is no recording online sessions or capturing of children’s images during the use of online platforms by any other person, unless specific and express consent has been received by the parent/guardian of the child
* Ensuring strict compliance with the service *Child Safe Environment Policy*
* Ensuring use of any online platform by children attending the service is an extension of the educational program and in line with the kindergarten’s educational philosophy.
* Ensuring children are educated about safe online practices at Elonera Pre School, at home and in the community
* Support and communicate with families about safe online practices at home and in the community

#### Parents/guardians are responsible for:

* reading and understanding this *Online Safety Policy*
* complying with all state and federal laws, the requirements of the *Education and Care Services* *National Regulations 2011*, and all service policies and procedures
* maintaining the privacy of any personal or health information provided to them about other individuals e.g. contact details.

#### Volunteers and students, while at the service, are responsible for following this policy and its procedures.

# Evaluation

In order to assess whether the values and purposes of the policy have been achieved, the Approved Provider will:

* regularly seek feedback from everyone affected by the policy regarding its effectiveness
* monitor the implementation, compliance, complaints and incidents in relation to this policy
* keep the policy up to date with current legislation, research, policy and best practice
* revise the policy and procedures as part of the service’s policy review cycle, or as required
* notify parents/guardians at least 14 days before making any changes to this policy or its procedures.

# Attachments

* Attachment 1: Procedures for use of online platforms with children at the service
* Attachment 2: eSafety Checklist for Early Learning Services
* Attachment 3: Parent/guardian authorisation for under-age access to online platforms via the use of Elonera Pre School ICT facilities

# Authorisation

This policy was adopted by the Elonera Pre School Committee of Management on 15 October 2020.

This policy was reviewed and approved by the Elonera Pre-School Committee of Management on 12 August 2021

# Review date: August 2022

**Attachment 1**

**Procedures for use of online platforms with children at the service**

* All online platforms should be age appropriate and meet specific educational/developmental objectives and early learning criteria
* Written or visual electronic communications exchanged through the use of online platforms with children must always be reviewed by an educator.
* Images of children in the kindergarten setting should not be published or distributed online unless specific and express written consent is provided by the child’s parent/guardian. Any such publication should be strictly within the scope of any consent provided.
* Use of online platforms by children attending the service is only permitted once the fully informed written consent of the child’s parent/guardian is received
* Use of online platforms by children attending the service must be closely supervised by an educator at all times
* No images or video or audio recordings should be captured by any means while children are using online platforms unless specific and express written consent is provided by the child’s parent/guardian. Any such use should be strictly within the scope of any consent provided.
* Where possible, use children’s first names only during the use of online platforms. Do not use surnames or other identifiers unless specific and express consent is provided by the child’s parent/guardian.
* No images of the children should be captured while using online platforms unless specific and express consent is provided by the child’s parent/guardian.
* Be cautious about opening files or launching programs that have been received as an attachment via an electronic communication. Instead, save an attachment to disk and scan with anti-virus software before opening, and keep an eye out for unusual filenames.
* Never open electronic communications if unsure of the sender.
* Users of online platforms at, on behalf of, or in collaboration with, Elonera Pre School 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
	+ carry out activities that are illegal, inappropriate or offensive to children, 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 online platforms 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
	+ exchange any confidential or sensitive information held by Elonera Pre School unless authorised as part of their duties
	+ 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.

### Information stored on computers

* Computer records containing personal, sensitive and/or health information, or photographs of children must be 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*).
* Computer 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.

**PERSONAL DEVICES:**

* Staff should not use personal devices to capture photos or videos of children or to facilitate the use of online platforms by children at the service.
* Families should not use personal devices such as phones and cameras to take pictures of children (other than their own) on the kindergarten premises or whilst participating in use of an online platform.

### Breaches of this policy

* Individuals who use online platforms 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 online platforms at the service 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 certain online platforms and the service’s ICT facilities restricted/denied.

**ATTACHMENT 2**

**eSafety Checklist for Early Learning Services**

https://www.esafety.gov.au/sites/default/files/2020-07/Checklist%20for%20Early%20Learning%20Services.pdf

**Attachment 3**

**Parent/guardian authorisation for under-age access to online platforms via the use of Elonera Pre School ICT facilities**

I, , [parent/guardian name] give permission for

 [child’s name] to use [insert online platform] for the purposes of [insert educational objective /developmental program] during my child’s attendance at Elonera.

I acknowledge that participation is optional and I have read the Elonera Pre School *Online Safety Policy* and agree to the conditions of use of the above online platform by my child.

Signature (parent/guardian) Date