Cybersafety – Policy QO172

RATIONALE

Ōtātara Children's Centre acknowledges that:

a) The internet, and Information and Communication Technologies (ICT) play an increasingly important role in children's learning, and in the administration of ECE services

b) The establishment and implementation of a cybersafety policy

  i) contributes to the provision of a safe learning environment which fosters children's emotional, physical and social development as described in the Education (Early Childhood Centres) Regulations 1998

  ii) contributes to the maintenance of a safe work environment and a safe environment for visitors under the Health and Safety in Employment Act 1992

  iii) assists Ōtātara Children's Centre to meet its obligations to deliver a curriculum which promotes the health of children, nurtures children's well-being, and keeps children safe from harm (Te Whāriki).

OBJECTIVES

This policy will assist Ōtātara Children's Centre to:

a) meet its legal obligations

b) provide guidance to centre staff and families/whānau and visitors regarding the safe and responsible use of ICT at or at activities relating to Ōtātara Children's Centre

c) educate members of the Ōtātara Children's Centre community regarding the safe and responsible use of ICT.

DEFINITION OF CYBERSAFETY

At Ōtātara Children's Centre we use the following definition of Cybersafety at the centre:

a) the safe and responsible use, at any time, on *or* off the centre site, by any person, of the *centre's* Internet facilities, network, and associated ICT equipment/devices, such as computers and laptops, digital cameras, mobile phones, and other devices.

b) the safe and responsible use by anyone, of any *privately-owned* ICT equipment/devices on the centre site, or at a centre-related activity.

CYBERSAFETY PRACTICES AT ŌTĀTARA CHILDREN'S CENTRE

1. **The Ōtātara Children's Centre programme of cybersafety includes:**
   a) This cybersafety policy
   b) Security systems which represent good practice including;
      i) updated anti-virus software
      ii) updated firewall software or hardware
      iii) updated anti-spyware software
      iv) regularly patched operating systems
      v) secure storage of ICT equipment/devices

2. **Permitted use**

   Use of the Ōtātara Children's Centre computer network, internet access, computers and other centre-owned ICT equipment/devices on or off the centre site, is restricted to:
   a) Centre staff.
   b) Whānau of enrolled children, students in the centre and/or other visitors who are authorised by the supervisor.
   c) Persons contracted to carry out work at the centre *and* at the discretion of the Supervisor such as trades people or technicians.
   c) For centre-related activities.
   d) Personal usage by centre staff (such as professional development) which is appropriate (see point 5) to the centre learning environment and is of a reasonable amount.

3. **Parents/caregivers consent for children to use ICT**

   The use of ICT equipment is a part of the curriculum at Ōtātara. Enrolment at the centre constitutes permission for children to be engaged in the use of such equipment unless otherwise agreed.

4. **Privately-owned/leased ICT equipment/devices**

   Use of *privately-owned* ICT equipment/devices (including mobile phones) at the centre or any centre-related activity is restricted to activities which are appropriate to the centre learning environment. This includes storage of any images or material on such devices.

5. **Appropriateness of use and content to Ōtātara Children's Centre learning environment**

   The Management team will provide guidance as to appropriate use in the centre learning environment, including the taking of photographs or video footage.

6. **User accounts and passwords**

   Access to the centre's computer network, computers, and Internet access, requires a password protected user account.

7. **Filtering and monitoring**
   a) EIT may utilise filtering and/or monitoring software where appropriate, to restrict access to certain websites and data, including email .
   b) EIT reserves the right to monitor, access, and review all use of centre-owned ICT equipment/devices. This includes personal emails sent and received using the centre's computers and/or network facilities, either during or outside centre hours.

8. **Ownership of electronic files or data**
   Any electronic data or files created or modified for the purpose of completing work on behalf of Ōtātara Children's Centre on any ICT, regardless of who owns the ICT, are the property of Ōtātara Children's Centre.

9. **Auditing**
   a) As the Licensee, EIT may, from time to time, at its discretion, conduct an audit of the computer network, Internet access facilities, computers and other centre ICT equipment/devices.
   b) Conducting an audit does not give any representative of Ōtātara Children's Centre the right to enter the home of centre personnel nor the right to seize or search any ICT equipment/devices belonging to that person.

10. **Inappropriate activities/material**
   a) Ōtātara Children's Centre and EIT will take all reasonable steps to filter or screen all material accessed using the centre's network or Internet access facilities. However, when using a global information system such as the internet, it may not always be possible for the centre to restrict access to all such material. This may include material which is **inappropriate** in the centre learning environment, **dangerous,** or **objectionable** as defined in the Films, Videos and Publications Classification Act 1993.
   b) While using the EIT network, Internet access facilities or ICT equipment/devices, **or using any privately-owned ICT equipment/devices at the centre or at any centre-related activity**, no person may:
      i) initiate access to, or have involvement with, inappropriate, dangerous, illegal or objectionable material or activities,
      ii) save or distribute such material by copying, storing or printing.
   c) Accidental access to inappropriate material:
      By parents, caregivers or other visitors:
      In the event of accidental access to any inappropriate material by a **family/ whānau member** or other visitor, a staff member should be consulted.
      Where the material is clearly of a more serious nature, or appears to be illegal, users should:
      i) remove the material from view (by closing or minimising the window, turning off the monitor, or shutting down the device),
      ii) report the incident immediately to a member of centre staff.

      By Centre Personnel:
      In the event of accidental access of inappropriate material at the lower range of seriousness (e.g. spam), **centre personnel** should delete the material.
      If the nature of such material is somewhat more serious, (e.g. spam containing inappropriate but not illegal images), delete it and report the issue to the management team who will keep a record of the incident. If uncertain as to the seriousness of the incident, the centre management should be consulted.
      When in doubt, log the incident.
      In the event of accidental access of inappropriate material clearly of a much more serious nature, or of material which appears to be illegal, users should:
      i) remove the material from view (by closing or minimising the window, or turning off the monitor)

ii) report the incident immediately to centre management who will keep a record of the incident and report the inappropriate site to the ICT support team so access to the site can be blocked.

11. Unauthorised software or hardware

Authorisation from the Supervisor must be gained before any attempts to download, install, connect or utilise any software or hardware onto or with any Ōtātara Children's Centre ICT equipment/devices. This includes use of such technologies as Bluetooth, infrared, and wireless, and any similar technologies which have been, or may be developed.

12. Children's use of the Internet and email.

a) Children will be actively supervised by centre personnel when accessing the Internet on the centre's site or at any centre-related activity.
b) Children may create and/or send email only under the active supervision of centre personnel.

13. Confidentiality and privacy

a) The principles of confidentiality and privacy extend to accessing or inadvertently viewing information about personnel, or children and their families, which is stored on the centre's network or any device
b) Privacy laws are such that centre personnel should seek advice from centre management regarding matters such as the collection and/or display/publication of images (such as personal images of children or adults), as well as text (such as children's personal writing)
c) Ministry of Education guidelines should be followed regarding issues of privacy, safety and copyright associated with the online publication of children's personal details or work.

14. Posting material

a) All material submitted for publication on the centre Internet/Intranet site should be appropriate to the centre's learning environment
b) Such material can be posted only by the authority of centre management
c) The centre management should be consulted regarding links to appropriate websites being placed on the centre's Internet/Intranet (or browser homepages) to provide quick access to particular sites.

15. Cybersafety training

Where personnel who supervise children's use of ICT indicate that they require additional training/professional development in order to safely carry out their duties, the Supervisor will consult with agencies which provide such training (such as NetSafe).

Document information – Office use only	
Document Name	Cybersafety
Document Number	QO172
Executive	Executive Director, Student and Academic Services
Owner	Executive Director, Student and Academic Services
Developer	Supervisor Children Centre
Review Frequency	12
Last Review	5/12/2023
Next Review	5/12/2024
Related Items	
Version history	New format July 2020 Migrated format March 2023