Computer and Cyber safety Policy

Enquiries to:	Manager, Chairperson, Board of Trustees
Applies to:	Kaiako, Parents, guardians, and tamariki
Date Developed:	June 2021
Date Reviewed:	July 2021
Date Approved:	
Next Review Date:	November 2022

References; MOE Regulations 2008, Licensing Criteria for ECE Centres HS32, Net safe, child protection, VCA

The Centre management endeavours to meet all its responsibilities as outlined in the ECE 2008 Regulations, Licensing Criteria and relevant legislation for the physical and emotional safety of the children attending its centre, and its responsibilities to employees and/or other personnel assisting in the running of the centre. This includes the need to establish and maintain the cyber safety of the centre environment.

This policy has been developed, and is designed to:

- educate teachers about cyber safety issues
- provide guidance regarding the safe and responsible use of ICT at LHCCC
- outline the nature of possible consequences associated with breaches of the LHCCC cyber safety policy, which may undermine the safety of the centre's environment.

References: www.netsafe.org.nz, 2008 MOE Regulations, Licensing Criteria, Child Protection

RATIONALE

1) The centre management of LHCCC acknowledges that:
   a) the Internet, and Information and Communication Technologies (ICT) play an increasingly important role in the learning of children in the ECE sector, and in the administration of ECE services
   b) the establishment and implementation of a cyber safety policy for CENTRE PERSONNEL AND PARENTS/WHANAU & CAREGIVERS:
      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 2008
      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
2) assists LHCCC to meet its obligations to deliver curriculum which promotes the health of children, nurtures children's well-being, and keeps children safe from harm as expressed in the Licensing Criteria and 2008 Ministry of Education Regulations

OBJECTIVES

This policy will assist LHCCC to:

a) meet its legal obligations as outlined in the previous section

b) provide guidance to teachers/staff, parents/whānau and visitors regarding the safe and responsible use of ICT at LHCCC or at related activities

c) educate members of the LHCCC community regarding the safe and responsible use of ICT.

DEFINITION OF CYBERSAFETY

Management uses the following definition of Cyber safety at the centre:

a) the safe and responsible operation/use, at any time, on *or* off the centre site, and 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 noted on the cover of this document

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.

Note that examples of a 'centre-related activity' include, but are not limited to, an excursion, or cultural event, *wherever its location*.

CYBER SAFETY PRACTICES AT LOWER HUTT CITY CHILDCARE AND EDUCATION CENTRE

1) The LHCCC programme of cyber safety

Management requires that the Centre Manager puts in place a cyber safety programme. This programme should include:

a) This cyber safety policy, for teachers/staff and parents/whānau

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

c) cyber safety education for educators and other personnel, children, and for the centre's community (e.g. Net Safe pamphlets, and Net Safe training modules developed specifically for the ECE sector).

d) It is imperative that everybody understands their responsibilities with respect to acceptable use if ICT.

2) Permitted use

Use of the LHCCC computer network, Internet access facilities, computers, and other centre-owned ICT equipment/devices (including mobile phones) on or off the centre site, is restricted to:

a) persons contracted to carry out work at the centre *and* at the discretion of the Centre Manager such as trades people or technicians

b) centre-related activities

c) personal usage by teachers (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 enrolment procedure clearly indicates that by enrolling their child, parents and caregivers agree to their child using or being involved with the use of ICT as part of the learning environment.

4) Privately-owned/leased ICT equipment/devices

Kaiko will not use private devices such as cell phones to take photos of videos of tamariki for documentation purposes. LHCCC provides cameras for this purpose.

5) Appropriateness of use and content to LHCCC learning environment

The Centre Manager will provide guidelines as to what is considered appropriate to the centre learning environment, including the taking of photographs or video. Personal work or data may not be stored on business computers.

6) User accounts and passwords

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

It is important that passwords are strong. It is recommended that a password:
a) uses a combination of upper- and lower-case letters, numbers and other characters
b) is a minimum of 8 characters in length
c) is changed regularly.

7) Filtering and monitoring

a) The centre may utilise filtering and/or monitoring software where appropriate, to restrict access to certain websites and data, including email

b) The centre 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. Computer equipment must not be removed from the centre premises without the prior approval of the centre manager.

8) Ownership of electronic files or data

Any electronic data or files created or modified for the purpose of completing work on behalf of LHCCC on any ICT, regardless of who owns the ICT, are the property of LHCCC. No staff should copy files or email files to an external address, save on a memory stick or CD for work on a non centre computer, i.e. home computer without the approval of the centre manager.

9) Auditing

a) The Board of Trustees may from time to time, at its discretion, but no obligation to do so, conduct an audit of its computer network, Internet access facilities, computers and other centre ICT equipment/devices.

b) Conducting an audit does not give any representative of LHCCC the right to enter the home of teachers/staff, nor the right to seize or search any ICT equipment/devices belonging to that person.

10) Performing work-related duties at home using privately-owned equipment/devices

Where it is necessary for teachers or parents/whānau to regularly perform centre-related duties (e.g. centre accounts or official correspondence) on privately-owned ICT equipment/devices at home, this work should be authorised by the centre manager outlining the work and the purpose.

11) Inappropriate activities/material

a) LHCCC 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 LHCCC 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 be involved 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 parents/whanau, or other visitor, a member of the Teaching team should be consulted.

Where the material is clearly of a more serious nature, or appears to be illegal, users should:

1. remove the material from view (by closing or minimising the window, turning off the monitor, or shutting down the device)
2. report the incident immediately to the Centre Manager.

By Kaiako

In the event of accidental access of inappropriate material at the lower range of seriousness (e.g. Spam), the centre manager 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 log the incident in writing to the centre Manager. If uncertain as to the seriousness of the incident, the centre management/Board 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:

1. remove the material from view (by closing or minimising the window, or turning off the monitor)
2. report the incident immediately to centre management who will take such further action as may be required under this policy.

Documentation will be kept file by the centre manger.

12) Unauthorised software or hardware

Authorisation from the centre manager must be gained before any attempts to download, install, connect or utilise any unauthorised software or hardware onto or with any LHCCC 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. Any user seeking authorisation should speak with the centre manager.

13) Children's use of the Internet and email.

a) Children will be actively supervised when accessing the Internet on the centre's site or at any centre-related activity

14) 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 teachers 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.

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. Permission for sharing on Edcua is signed for by parent on the enrolment form.

15) Posting material

a) All material submitted for publication on the centre Internet site should be appropriate to the centre's learning environment

b) Such material can be posted only by those given the authority to do so by the centre management

c) The centre management should be consulted regarding links to appropriate websites being placed on the centre's Internet (or browser homepages) to provide quick access to particular sites.

d) Involvement as a representative of LHCCC with any non-centre website including Facebook must be with the approval of the centre management.

e) Photos of children to be posted in the website will have signed parent permission.

16) Cyber safety training

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

17) Breaches of this policy

a) Breaches of this policy can undermine the values of the centre and the safety of the learning environment

b) Any breach which is deemed harmful to the safety of the centre (for example, involvement with inappropriate material, or the use of ICT to facilitate anti-social behaviour such as harassment), may constitute serious misconduct. The centre will respond to any breach of the use agreement in an appropriate manner, taking into account all relevant factors, including any enrolment agreement, and any contractual and/or statutory obligations

c) If there is a suspected breach of this policy involving privately-owned ICT on the centre site or at a centre-related activity, the matter may be investigated by the centre Manager and the Board. The centre may request permission to audit that equipment/device(s) (This includes personal cameras, the centre provides cameras for centre use only).

d) Any breach concerning involvement with material which is deemed 'age-restricted', or 'objectionable' under the Films, Videos and Publications Classification Act 1993, is a very serious matter. In such situations, it may be necessary to involve law enforcement agencies in addition to any response made by the centre as a result of its investigation

e) The centre manager is required to immediately report to the Board of trustees any serious cybersafety incident or issue that has arisen.

18) Reporting to Board of Trustees

The centre manager is required to make regular reports to the Boad of trustees. Included in these reports should be the cyber safety measures LHCCC has in place, any professional development requirements, and any issues or incidents which have arisen since the previous report and did not require immediate reporting at the time, and any recommendations.

19) Use of Social Network Websites

All employees are asked to use great care when posting information on Facebook, and other social network websites. You are not permitted to use the name of the Centre, in any format, or in any context without the express permission of the Centre Manager. You are not permitted to refer to any employee, child, or parent of any child at the Centre except to the extent that the employee/child may be known to you socially. Adverse comments about the Centre, your colleagues, any child in your care, or any parent or any images that bring the Centre into disrepute may place you in breach of your employment agreement.

Emails

Employees may not send messages which are abusive, defamatory or which make discriminatory reference to a person's race, colour, religion, creed, sex, national origin, age, marital status sexual orientation, or disability, or that may otherwise constitute harassment. Employees must follow good email etiquette – keep messages short and to the point, answer promptly and not use language or punctuation that is open to misinterpretation. Ensure abrupt emails are not sent in the heat of the moment; allow a cooling down period before responding. (Professionalism at all times). Messages should reflect the values and standards of the Centre.

20) Policy review

The centre mangement will review this policy annually or in the event of new legislation.

Board of Trustees consulted	Yes/No	Kaiako consulted	Yes/No
Parents consulted	Yes/No		
Approved by: _____		Designation:_____	Date:_____