Cyber-Safety Policy

Rationale:

1) The management of Little Explorers 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 cybersafety policy and cybersafety use agreements for centre personnel AND parents/whanau:
      i) Ensures that Little Explorers takes all reasonable steps to promote that good health and safety of the children enrolled in the service. Regulation 46, 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
      iii) Little Explorers takes all practical steps to protect children from exposure to inappropriate material. HS32.
2) The policy document and related use agreements are not intended to be exhaustive documents containing all relevant rights and obligations that may exist in legislation to regulate use, storage and dissemination of information.

Objectives:

This policy will assist Little Explorers to:

a) meet its legal obligations as outlined in the previous section
b) provide guidance to centre personnel, parents/whanau, and visitors regarding the safe and responsible use of ICT at Little Explorers or at every centre related activity
c) educate members of the Little Explorers community regarding the safe and responsible use of ICT.

Definition of cybersafety:

The management uses the following definition of Cybersafety 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, iPads 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, a field trip, camp, sporting or cultural event, *wherever its location*.

Cybersafety practices at Little Explorers:

1) The Little Explorers programme of cybersafety

The Management requires that the supervisor puts in place a cybersafety programme. This programme should include:

a) This cybersafety policy, and comprehensive use agreements for centre personnel and parents/whanau
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) cybersafety education for educators and other personnel, children, and for the centre's community (e.g. NetSafe pamphlets, and NetSafe training modules developed specifically for the ECE sector).

2) Permitted use

Use of the Little Explorers 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) Centre Personnel who have signed a cybersafety use agreement

b) Parents/Whānau of enrolled children, and/or other visitors who have signed the appropriate Little Explorers cybersafety use agreement

c) Persons contracted to carry out work at the centre *and* at the discretion of the Management Team such as trades people or technicians

d) centre-related activities

e) personal usage by centre personnel (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

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 Little Explorers learning environment

The management will provide guidelines as to what is considered appropriate to the centre learning environment, including the taking of photographs or video.

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.

8) Ownership of electronic files or data

Any electronic data or files created or modified for the purpose of completing work on behalf of Little Explorers on any ICT, regardless of who owns the ICT, are the property of Little Explorers.

9) Auditing

a) The Management may from time to time, at its discretion, 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 Little Explorers 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) Performing work-related duties at home using privately-owned equipment/devices

Where it is necessary for centre personnel or parents/whanau 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 management team.

Inappropriate activities/material

a) Little Explorers 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 Little Explorers 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 **parent/whanau**, or other visitor, a member of the management 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 a member of management.

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 also log the incident in the ICT Incident Book*. 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:

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.

* The ICT Incident Book is to be kept by management.

11) Unauthorised software or hardware

Authorisation from management must be gained before any attempts to download, install, connect or utilise any unauthorised software or hardware onto or with any Little Explorers 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 management.

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

a) Children will be actively supervised by centre personnel, or by someone who has signed an Little Explorers cybersafety use agreement 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 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/Intranet (or browser homepages) to provide quick access to particular sites

d) Involvement as a representative of Little Explorers with any non-centre website must be with the approval of the centre management.

15) Cybersafety 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).

16) 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. The centre may request permission to audit that equipment/device(s)

d) If an incident is being investigated in which use of centre ICT by any person who does *not* have a signed use agreement with the centre includes some level of involvement by centre personnel, the extent of the centre personnel responsibility will be assessed by the management team.

e) 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

f) The Supervisor is required to immediately report to the Manager any serious cybersafety incident or issue arising from the situations detailed in (e).

17) Policy review

The management will review this policy annually.

Approved: 01/08/2011
Last Reviewed: 08/04/2014