April 2009: Copyrighted NetSafe® Sample Cybersafety Policy for New Zealand ECE Services

Administration Page

This page is *for information only*, and is intended to assist the person responsible for distributing the attached document.

This policy template is also distributed in a combined form together with NetSafe cybersafety use agreements for ECE personnel. It is recommended that services wishing to implement use agreements in conjunction with a cybersafety policy, download the combined document from www.netsafe.org.nz. A use agreement template for parents and caregivers is also available from the same site.

This download contains:

- This information page for administration use only
- A cover sheet for the policy
- A cybersafety policy template

Suggested procedure:

1. Read through this entire document before taking any further action
2. It is recommended that time be set aside to explain to all relevant service personnel (e.g. the licensee, educators, committee members, and other relevant people) the reasons why this policy has been developed
3. At the above meeting, distribute copies of the policy template and go over the contents. Ask for feedback, allowing sufficient time to take the document away and read it carefully. You should make it clear that during this time, any queries or concerns can be raised and discussed
4. Following feedback, personalise the template to suit the individual circumstances of your ECE service (see below for important notes regarding personalisation)
5. Ratify the personalised *Cybersafety Policy* following the usual process at your service
6. Distribute copies of the newly personalised policy to personnel. You should make it clear that personnel are always welcome to raise queries with management.

Personalising the templates

The terms within [ ] are designed to be modified to suit the individual details and nature of your service. The term 'personnel', for instance, may not apply in your circumstance. For clarification, the following indicates who or what each term is intended to cover:

[EVERY CENTRE]	The name of your service
[LICENSEE/COMMITEE]	The individual or group having responsibility for setting policy
[HEAD TEACHER/MANAGER]	The person responsible for the day-to-day running of the ECE service
[CENTRE PERSONNEL]	Educators, teachers and other staff employed by your service. Depending on the nature of your service, this term may also be used to cover other people such as full time volunteers. In many such circumstances these will be parents, caregivers or legal guardians of children at the centre. It is suggested that where such a person assists in the centre on a regular rather than occasional basis, they be asked to sign the centre personnel use agreement rather than the agreement for parents and guardians. This helps to ensure *regular* helpers are more adequately informed about the service's cybersafety policy and their responsibilities under it
[PARENTS/CAREGIVERS]	Parents, legal guardians or caregivers of children enrolled at the ECE service

Recommendation to obtain legal advice before personalising some wording

This template has been subject to consultation with a number of organisations and professionals within the ECE sector, and also with lawyers specialising in the field of education, as well as ICT and forensic specialists. It is strongly recommended that alterations to the following sections, in particular, are made only after obtaining independent legal advice:

Policy sections: 9, 10, 17c. (note also that point 3 may require modification to enrolment documents)

CYBERSAFETY AT [EVERY CENTRE]

CYBERSAFETY POLICY

The Internet, and Information and Communication Technologies (ICT) play an increasingly important role in children's learning, and in the administration of ECE centres.

The [LICENSEE/COMMITTEE] of [EVERY CENTRE] endeavours to meet all its responsibilities as outlined in the [CHARTER/LICENCE] 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 cybersafety of the centre environment.

This policy has been developed as part of the [EVERY CENTRE] cybersafety programme, and is designed to:

- educate [CENTRE PERSONNEL] about cybersafety issues
- provide guidance regarding the safe and responsible use of ICT at [EVERY CENTRE]
- outline the nature of possible consequences associated with breaches of the [EVERY CENTRE] cybersafety policy, which may undermine the safety of the centre's environment.

Important terms used in this document:

(a) *The abbreviation **'ICT'** in this document refers to the term 'Information and Communication Technologies'.*

(b) ***'Cybersafety'** refers to the safe and responsible use of the Internet and ICT equipment/devices, including mobile phones.*

(c) ***'Centre ICT'** refers to the centre's computer network, Internet access facilities, computers, and other centre ICT equipment/devices as outlined in (d) below.*

(d) *The term **'ICT equipment/devices'** used in this document, includes but is not limited to, computers (such as desktops, laptops, PDAs), video game consoles, storage devices (such as USB and flash memory devices, CDs, DVDs, floppy disks, iPods, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, video and audio players/receivers (such as portable CD and DVD players), and any other, similar, technologies as they come into use*

(e) *'**Objectionable'** in this context means the definition used in the Films, Videos and Publications Classification Act 1993. All objectionable material is illegal, and can include such material as images of child sexual abuse, extreme violence, and extreme cruelty.*

*Some material such as pornography (of a type similar to that which can be legally purchased from video or magazine outlets), may be classified as '**restricted'**. Although the material itself may not be illegal, it **is illegal** to supply restricted material to people under a certain age.*

[EVERY CENTRE] Cybersafety Policy

RATIONALE

1) The [LICENSEE/COMMITTEE] of [EVERY CENTRE] 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 & 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 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 [EVERY CENTRE] 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 Revised Statement of Desirable Objectives and Practices for Chartered Early Childhood Services in New Zealand (DOPs) 1996.

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 [EVERY CENTRE] to:

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

   b) provide guidance to [CENTRE PERSONNEL], [PARENTS/CAREGIVERS], and visitors regarding the safe and responsible use of ICT at [EVERY CENTRE] or at [EVERY CENTRE] related activities

   c) educate members of the [EVERY CENTRE] community regarding the safe and responsible use of ICT.

DEFINITION OF CYBERSAFETY

The [LICENSEE/COMMITTEE] 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, 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 [EVERY CENTRE]

1) The [EVERY CENTRE] programme of cybersafety

The [LICENSEE/COMMITEE] requires that the [HEAD TEACHER/MANAGER] puts in place a cybersafety programme. This programme should include:

   a) This cybersafety policy, and comprehensive use agreements for [CENTRE PERSONNEL] and [PARENTS/CAREGIVERS]

   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 [EVERY CENTRE] 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/CAREGIVERS] of enrolled children, and/or other visitors who have signed the appropriate [EVERY CENTRE] cybersafety use agreement

c) Persons contracted to carry out work at the centre *and* at the discretion of the [HEAD TEACHER/MANAGER] 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 [EVERY CENTRE] learning environment

The [HEAD TEACHER/MANAGER] 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 [EVERY CENTRE] on any ICT, regardless of who owns the ICT, are the property of [EVERY CENTRE].

9) Auditing

a) The [LICENSEE/COMMITTEE] 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 [EVERY 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) Performing work-related duties at home using privately-owned equipment/devices

Where it is necessary for [CENTRE PERSONNEL] or [PARENTS/CAREGIVERS] 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 [LICENSEE/COMMITTEE].

11) Inappropriate activities/material

a) [EVERY CENTRE] 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 [EVERY CENTRE] 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/CAREGIVER]**, or other visitor, a member of the [CENTRE PERSONNEL] 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 [CENTRE PERSONNEL].

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 the [HEAD TEACHER/MANAGER]

12) Unauthorised software or hardware

Authorisation from [HEAD TEACHER/MANAGER] must be gained before any attempts to download, install, connect or utilise any unauthorised software or hardware onto or with any [EVERY 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. Any user seeking authorisation should speak with the [HEAD TEACHER/MANAGER].

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

a) Children will be actively supervised by [CENTRE PERSONNEL], or by someone who has signed an [EVERY CENTRE] 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].

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 [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.

15) 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 [EVERY CENTRE] with any non-centre website must be with the approval of the centre management.

16) 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 [HEAD TEACHER/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. 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 [HEAD TEACHER/MANAGER] and/or [LICENSEE/COMMITTEE]

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 [HEAD TEACHER/MANAGER] is required to immediately report to the [LICENSEE/COMMITTEE] any serious cybersafety incident or issue arising from the situations detailed in (e).

18) Reporting to [LICENSEE/COMMITTEE]

The [HEAD TEACHER/MANAGER] is required to make regular reports to the [LICENSEE/COMMITTEE]. Included in these reports should be the cybersafety measures the [EVERY CENTRE] 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) Policy review

The [LICENSEE/COMMITTEE] will review this policy annually.

Signed: Date:

Role (e.g. Licensee/Committee Chair): Date for review:
