Aspiring Beginnings Early Learning Centre
Cybersafety policy
Reference: Regulation 43, HS31-32, ECECF 2008

The Internet, and Information and Communication Technologies (ICT) play an increasingly important role in children's learning, and in the administration of ECE centres. Teachers have a pivotal role in developing the attributes of cybercitizenship in children. Cybercitizenship implies that users of technology are safe, confident and act with integrity. A Cybersafe learning environment is one where ICT is used safely and responsibly to support effective learning and teaching.

The Governance committee of ABELC endeavours to meet all its responsibilities as outlined in the charter 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. We understand that children in ECE have not developed the understanding and judgement to use this type of technology safely and responsibly, and therefore are particularly vulnerable to potential risks. The teachers and staff need to be aware of the extent to which their own use is observed by children, and guided by the "Net Basics" philosophy as set down by the Ministry of Education. This includes the need to establish and maintain the cybersafety of the centre environment.

This policy has been developed as part of the ABELC cybersafety programme, and is designed to:

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

This consists of 3 different sections:

- Cybersafety Policy
- Cybersafety Use Agreement for parents/caregivers
- Cybersafety Use Agreement for all employees of the centre

Important terms and definitions used in this document:

(a) Aspiring Beginnings Early Learning Centre is referred to 'ABELC' in this document

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

(c) Cybersafety' is referred to
- *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.*
- *the safe and responsible use by anyone, of any privately-owned ICT equipment/devices on the centre site, or at a centre-related activity.*

(d) "Cybercitizenship' refers to the users of technology acting with integrity and are safe & confident users.

(e) 'Cybernetworking' refers to the collaborative approach to the sharing of cyber information in a safe and responsible manner.

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

(g) 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, electronic equipment and associated technologies. as they come into use.

(h) centre-related activity' include, but are not limited to, an excursionp, camp, sporting or cultural event, wherever its location.

(i) '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.*

RATIONALE

1) The Governance committee of ABELC 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 staff 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 ABELC 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 Education (Early Childhood Services) Regulations 2008.
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 ABELC to:

a) meet its legal obligations as outlined in the previous section
b) provide guidance to staff, parents/caregivers and visitors regarding the safe and responsible use of ICT at ABELC or at centre related activities
c) educate members of the ABELC community regarding the safe and responsible use of ICT.

CYBERSAFETY PRACTICES

1) The ABELC programme of cybersafety

The governance committee requires that the Senior Teacher puts in place a cybersafety programme. This programme should include:

a) This cybersafety policy, and comprehensive use agreements for;
    i) Employees of the centre
    ii) Parents/Caregivers, and Whanau if necessary
    iii) Other visitors who have been requested to sign the appropriate cybersafety use agreement.
b) Security systems which represent good practice including;
    i) appropriately password protecting all computers
    ii) updated anti-virus software
    iii) updated firewall software or hardware
    iv) updated anti-spyware software
    v) regularly update operating systems
    vi) secure storage and care of ICT equipment/devices
c) Cybersafety education for teachers and staff, children, and for the centre's community (e.g. NetSafe pamphlets, and NetSafe training modules developed specifically for the ECE sector including NetSafe website).

2) Permitted use

Use of the ABELC 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) staff who have signed a cybersafety use agreement

b) parents/caregivers of enrolled children, and/or other visitors who have signed the appropriate ABELC cybersafety use agreement

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

d) centre-related activities

e) Personal usage by 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

By completing the enrolment contract when enrolling their child, parents/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 ABELC learning environment

The Senior teacher 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

a) Any electronic data or files created or modified for the purpose of completing work on behalf of ABELC on any ICT equipment, *regardless of who owns the ICT*, are the property of ABELC.

b) Under no circumstances is data to remain stored on privately-owed ICT equipment. ABELC may therefore request that such files/data be returned or delivered to ABELC and/or be deleted from your personal ICT equipment.

9) Auditing

a) The Governance 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 ABELC the right to enter the home of 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 staff, parents/caregivers, and governance committee members to regularly perform centre-related duties on privately-owned ICT equipment/devices at home, this work must first be authorised by the Governance committee.

11) Inappropriate activities/material

a) ABELC 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 ABELC 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:

For parents/caregivers:

In the event of accidental access to any inappropriate material by a parent/caregiver or other visitor, a member of the staff must 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 staff.

For employees:

In the event of accidental access of inappropriate material by an employee at the lower range of seriousness (e.g.Spam), it should be deleted immediately.

If the nature of such material is somewhat more serious, (e.g. spam containing inappropriate but not illegal images), delete it and advise the office so the incident can be logged. 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 take such further action as may be required under this policy.

12) Unauthorised software or hardware

Authorisation from centre management must be gained before any attempts to download, install, connect or utilise any unauthorised software or hardware onto or with any ABELC 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 Senior Teacher.

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

a) Children will be actively supervised by staff who have signed an ABELC cybersafety agreement when accessing the Internet on the centre's site or at any centre-related activity. Staff will also supervise others who have signed an ABELC cybersafety use agreement. If an agreement has not been signed authorisation is not given to use the internet.

b) Children may create and/or send email only under the active supervision of teachers.

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 all staff 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 approval from 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 ABELC with any non-centre website must be with the approval of the centre management.

16) Cybersafety training

a) To ensure employees feel confident that they can safely supervise children's use of ICT equipment, they will take all measures to familiarise themselves with appropriate practices for cybersafety education for teachers and staff, children, and for the centre's community, via NetSafe pamphlets and NetSafe training modules developed specifically for the ECE sector. This information is available from the MOE NetSafe website (www.netsafe.org.nz).

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 staff, the extent of the staff responsibility will be assessed by the Senior Teacher and/or Governance 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 Senior Teacher is required to immediately report to the Governance committee any serious cybersafety incident or issue arising from the situations detailed in (e).

18) Reporting to Governance committee

The Senior Teacher is required to make regular reports to the Governance committee. Included in these reports should be the cybersafety measures the ABELC has in place, any professional development requirements, and any issues or incidents which have arisen since the previous report and did not require.

Signed:		Next review:	Dec 2014	_____
Role:	Governance		Dec 2015	_____
Date:	February 2014		Dec 2016	_____

Parents/caregivers handout:

Cybersafety Use Agreement for Parents/Caregivers

From time to time, Parents/caregivers may have the opportunity to use ABELC Internet facilities, network and other ICT devices such as mobile phones, digital cameras or computers. This may arise while visiting the centre, at a centre activity off-site, or through the lending of ABELC ICT to children and families enrolled at the centre.

Our policy is that every adult must have signed a cybersafety use agreement before using the *centre's ICT* while visiting the centre, at a centre event, or borrowing any of centre's ICT equipment/devices.

The use agreement also contains guidelines covering the appropriate use of *privately-owned* ICT devices such as mobile phones while at ABELC.

The agreement is based upon the ABELC Cybersafety Policy, which is filed in the policies & procedure manual located in the centre foyer or can be downloaded from our centre website.

We ask that all parents and caregivers who visit our centre, sign the following use agreement.

This helps to ensure that all use of ICT at ABELC is done so with knowledge of the centre's cybersafety programme and its aims.

If you have a query regarding this use agreement or our cybersafety policy, please feel free to discuss it with centre management before signing the acknowledgement.

Parents/caregivers handout:

CYBERSAFETY RULES AND RESPONSIBILITIES

What can the centre's ICT equipment be used for?

If permission has been given to use the centre's computer network, Internet access facilities, computers and other centre-owned ICT equipment (including mobile phones) on or off the centre site, they are to be used for ***centre-related activities only.***

Can I use my own ICT equipment (e.g. laptop, digital camera, mobile phone) at ABELC?

You may use privately-owned ICT equipment (including mobile phones) on the centre site or at any centre-related activity, provided that use is appropriate to the centre's learning environment.

Any images or material present or stored on privately-owned ICT equipment brought onto the centre site or to any centre-related activity must be appropriate to the centre's learning environment. This includes images and text stored on mobile phones.

What material or activities are appropriate to the centre's learning environment?

The centre management should be consulted beforehand where you are unsure if particular material or a particular activity is appropriate in a learning environment for young children.

Can I take photographs or video at ABELC?

The centre management must be consulted before you take any photographs, video, or any other recordings using any device while at the centre or any centre-related activity.

ABELC may ask to view any such recordings and request they be deleted.

What about access to, or involvement with, inappropriate or illegal material or activities?

When using centre ICT at any time, or privately-owned ICT at the centre or at any centre-related activity, you must not:

- initiate access to, or have involvement with, inappropriate or illegal material or activities
- save or distribute such material by copying, storing, printing or uploading to social media.

What about passwords?

Any passwords supplied to you should be kept confidential and not shared with anyone else.

Can I use email at ABELC?

If permission has been given to use ABELC e-mail accounts, it must be done so in an appropriate and responsible manner, and only after consultation with centre management.

You must not use ABELC facilities to access or send personal email not associated directly with centre activities.

How is the privacy of my family's information protected?

While using the centre's ICT equipment/devices parents/caregivers must not, unless directed by centre management, actively seek or search for information or data relating directly to other enrolled families.

Can I install my own software onto ABELC ICT?

You must not attempt to download, install, connect or utilise any unauthorised software or hardware onto or with any ABELC ICT equipment.

What if I carry out work for ABELC on my own ICT such as my home computer?

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

ABELC may therefore request that such files/data be returned or delivered to ABELC and/or be deleted from your personal equipment.

What do I do if I have any query regarding this agreement or the cybersafety policy?

If you have any query regarding the cybersafety use agreement or the cybersafety policy you should contact the centre management as soon as possible.

To be completed by parents/caregivers and returned:

ACKNOWLEDGEMENT OF ABELC CYBERSAFETY RULES AND RESPONSIBILITIES
Aspiring Beginnings Early Learning Centre

To the Parent/Legal Guardian/Caregiver:

1. Please read this page carefully as it includes information about your responsibilities under this agreement.
2. Complete and sign the section at the bottom of the page.
3. Return this acknowledgement page to the centre (a copy will be returned to you).
4. Keep your copy of the Cybersafety Use Agreement for parents/caregivers for future reference.

ABELC will:

1. do its best to enhance learning through the safe use of ICT. This includes working to restrict access to inappropriate, illegal or harmful material on the internet or centre ICT equipment/devices at the centre or at centre- related activities
2. respond to any breaches in an appropriate manner
3. welcome enquiries from parents/legal guardians/caregivers about cybersafety issues.

I acknowledge that:

- I have read the *ABELC Cybersafety Use Agreement for parents/caregivers*
- I am aware that I can request a copy of the *ABELC Cybersafety Policy or view it on the centre website*
- I have read and am aware of the rules and responsibilities outlined in the Cybersafety Use Agreement, a copy of which I have been advised to retain for reference
- I am aware that these obligations and responsibilies relate to the safety of the children attending the centre, and of the centre's learning environment.
- I believe that I have sufficient knowledge to safely supervise the use made by children in my care, of the centre's computer network, Internet access facilities, computers, webcams and other centre ICT equipment/devices.

I also understand that breaches of this Use Agreement will be investigated and may require a response by ABELC centre management or governance committee.

Child's Name (print): .....

My Name (print): .....

Parent/Legal Guardian/Caregiver (please circle which term is applicable)

Signature: ..... Date: .....

Name of additional signatory* (if applicable): .....

Parent/Legal Guardian/Caregiver (please circle which term is applicable)

Signature: ..... Date: .....

** Additional Parents/caregivers of the same child, may also sign the agreement. This will avoid the necessity to sign a separate agreement should the additional parents/caregivers visit the centre or use the centre ICT infrequently.*

Staff handout:

CYBERSAFETY USE AGREEMENT FOR ALL EMPLOYEES
Aspiring Beginnings Early Learning Centre

Rules and Responsibilities

1) Use of the ABELC 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) Only staff who have signed a cybersafety use agreement
   b) enrolled children whose parents/caregivers have signed a cybersafety use agreement
   c) parents/caregivers of enrolled children, and/or other visitors who have signed a cybersafety use agreement
   d) Persons contracted to carry out work at the centre *and* at the discretion of the senior teacher such as trades people or technicians
   e) centre-related activities
   f) personal usage by teachers and staff that is appropriate to the centre learning environment and of a reasonable amount.
2) 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 rule includes any stored images or material brought to the centre or any centre-related activity, on any device.
3) Any staff who have a signed use agreement with the centre, and who allow another person (with the exception of a contractor) *who does not have a signed use agreement with the centre* to use centre ICT, are responsible for that use.
4) When using centre ICT at any time, or privately-owned ICT at the centre or at any centre-related activity, users must not:
   - initiate access to, or have involvement with, inappropriate or illegal material or activities
   - save or distribute such material by copying, storing, printing or uploading to social media.
5) Any incident involving inappropriate material or activities of a serious nature, or suspected of being illegal, must be reported immediately to the Senior Teacher and/or governance committee.
6) Passwords must be kept confidential and not shared with anyone else.
7) Users should not allow another person access to any equipment/device logged in under their own user account, unless as part of authorised work being carried out on the centre network or ICT equipment/devices.
8) ABELC e-mail accounts are expected to be used in a responsible manner and in accordance with this use agreement. This includes ensuring that no electronic communication could cause offence to, harass, or harm others, put the owner of the user account at potential risk, bring the centre into disrepute, or in any other way be inappropriate in the centre's learning environment.
9) For personal safety, users should be very careful about revealing personal information about themselves, such as home or email addresses, or any phone numbers including mobile numbers. Nor should such information be passed on about others.
10) All centre ICT equipment/devices should be cared for in a responsible manner and stored safely when not in use, especially when the centre is not operating.
11) Any damage, loss or theft must be reported immediately to the Senior Teacher or if necessary directly to the governance committee.
12) All users are expected to practise sensible use to limit wastage of computer resources or bandwidth. This includes avoiding unnecessary printing, and unnecessary Internet access, uploads or downloads.

13) Authorisation from senior teacher/administration must be gained before any attempts to download, install, connect or utilise any unauthorised software or hardware onto or with any ABELC ICT equipment/devices.

14) Where permission has been given to connect or install privately-owned equipment/devices or software, it is with the understanding that the centre may scan this equipment/device/software at any time thereafter as part of a regular or targeted security check, such as for viruses.

15) Copyright laws and licensing agreements must be respected. This means no involvement in activities such as illegally copying material in any format, copying software outside of the terms of the licence, downloading copyrighted video or audio files, using material accessed on the Internet in order to plagiarise, or illegally using unlicensed products.

16) Authorisation from Centre Management must be gained before submitting any material for publication on the centre Internet/Intranet site.

17) Children will be actively supervised by teachers, or by someone who has signed an ABELC cybersafety use agreement when accessing the Internet on the centre's site or at any centre-related activity.

18) Personnel should seek advice from the Senior Teacher regarding matters such as the online collection and/or display/publication of personal information in any form. This includes personal data, images of children or adults, and text, such as children's personal writing.

19) All employees will ensure they keep themselves familiar with current Netsafe practises as outline on Netsafe correspondence available in hard copy on via the MOE website.

20) Unacceptable use while at the centre:

    a) Use of the internet and e-mail is for Aspiring Beginnings purposes **only**, unless otherwise authorised by management.

    b) Centre Management reserves the right to check or monitor all internet and e-mail messages.

    c) The internet and e-mail may not be used for the following;

        i) Commercial gain and personal business use

        ii) Any illegal or malicious purpose

        iii) Using objectionable or abusive language, or messages to criticise or malign a person at the centre

        iv) Creating / sending and down-loading information which is objectionable in nature, such as pornographic or other material which is in poor taste

        v) Creating or responding to electronic mail chain letters

    d) Misrepresenting Aspiring Beginnings and doing or saying anything which brings the centre, or anyone directly involved with the centre, into disrepute

    e) Activities which cause congestion or disruption to networks and systems, such as playing games at any time or down-loading amounts of information during work hours

    f) To prevent viruses, staff must never open any pop-up unsolicited windows

    g) Down-loading games

    h) Disciplinary action will be taken for any breach of the above where the staff member(s) concerned are unable to provide an acceptable explanation. Such action may include the removal of internet access or the use of the computers. Staff may also be billed with the cost of reformatting or reinstating any Aspiring Beginnings computer programmes or systems damaged as a result of any of the ABELC above.

To be completed by employee:

ACKNOWLEDGEMENT OF ABELC RULES AND RESPONSIBILITIES
Aspiring Beginnings Early Learning Centre

Please complete, sign, and date this employee Use Agreement Form which confirms your agreement to follow the obligations and responsibilities outlined in this document.

If you have any queries about the agreement, you are encouraged to discuss them with the centre management before you sign and return this page to centre management.

A copy of the signed form will be supplied to you.

Use Agreement

I acknowledge that I have read a copy of the ABELC Cybersafety Policy. I have read and am aware of the obligations and responsibilities outlined in this staff Cybersafety Use Agreement document, a copy of which I have been advised to retain for reference. These obligations and responsibilities relate to the cybersafety of the children attending the centre, and of the centre's learning environment.

I also understand that breaches of this Use Agreement will be investigated and may require a response by ABELC centre management, which could include, where necessary, referral to a law enforcement agency.

Name: .....

Role in the centre: .....

Signature: .....

Date: .....