GROW Excellence in Care and Education	**Policy**
	Policy Category: HEALTH AND SAFETY
	Date Created: November 2016
	Policy Name: HS32 Cyber Safety Policy

Purpose

The purpose of this operational policy is to keep children and adults safe by meeting Licensing Criteria HS32.

Position Statement

This centre does everything possible to keep children and adults in our centre safe whilst using ICT equipment and technology. This means all practicable steps are taken to protect children from exposure to inappropriate material. It also means practising ethical digital citizenship.

Issue Outline

Cyber Safety is the safe, ethical, and responsible use of Information and Communication Technologies (ICT).

It is important that we protect ourselves and the centre's ICT system from viruses, spam and other inappropriate content.

The use of digital technologies and the Internet provides an almost unlimited educational resource and a facility to communicate, display and revisit the results of our work, engage in research, assessment and professional development. It is imperative that everybody understands their responsibilities with respect to acceptable use of ICT.

Detail

General:

- Staff are made aware of the need for online safety and the nature of the possible threats that could be encountered whilst engaging in activity through the Internet, e.g. security threats, protecting and managing personal data, and avoiding harmful or illegal content.
- Staff will be made aware of the centre's safe internet practices, e.g. password use and other safety practices specific to the centre.
- All centre computers and laptops that have access to the internet shall be password protected. Only centre staff and authorised personnel shall have access to the password.
- All use of ICT equipment and technology at our centre for administration, assessment or teacher education (e.g. PD and research) purposes is conducted away from teaching spaces
- Only ICT equipment and technology owned or leased by the Centre may be used in our Centre and as part of our programme. Staff are not to use their personal laptops, mobile phones or other ICT equipment for teaching purposes.

- Staff members may make personal use of their own and /or centre ICT equipment, internet and email access provided this takes place during non-contact or break times away from teaching spaces, is within reasonable limits, does not result in a cost to the centre and does not place the centre at risk.
- All use of ICT equipment and technology for teaching purposes at our centre will be planned and supervised.
- If ICT equipment is used for educational purposes, safeguarding procedures will be in place to ensure children are not exposed to inappropriate or harmful material.
- Teachers will take all practical steps to ensure inappropriate or objectionable material (as defined by the Films, Videos and Publications Classification Act 1993) is not accessed at any time at our centre.
- Accidental or intentional breaches of this policy by staff will be treated as a serious misconduct issue
- The centre will ensure appropriate virus, spyware and malware protections are available and in place

Filtering and monitoring

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

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.

Ownership of electronic files or data

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

Auditing

The licensee 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.

Conducting an audit does not give any representative of Grow Early Education the right to enter the home of Centre personnel, nor the right to seize or search any ICT equipment/devices belonging to that person.

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

Where it is necessary for Centre personnel 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 Manager.

Inappropriate activities/material

Grow Early Education 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.

While using the Grow Early Education 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

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 inform the centre manager. If uncertain as to the seriousness of the incident, the centre management should be consulted.

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.

Unauthorised software or hardware

Authorisation from the Manager must be gained before any attempts to download, install, connect or utilise any unauthorised software or hardware onto or with any Grow Early Education ICT equipment/devices. This includes use of such technologies such as Bluetooth, infrared, and wireless, and any similar technologies which have been, or may be developed. Any user seeking authorisation should speak with the Manager.

Children's use of the Internet and email.

Children will be actively supervised by Grow Early Education, or by someone who has signed a Grow Early Education cyber safety use agreement when accessing the Internet on the centre's site or at any centre-related activity

Children may create and/or send email only under the active supervision of Centre Personnel.

Confidentiality and privacy

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

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)

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.

Posting material

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

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

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

Involvement as a representative of Grow Early Education with any non-centre website must be with the approval of the centre management.

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/supervisor will consult with agencies which provide such training (such as NetSafe).

Breaches of this policy

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

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

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)

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 Manager and/or Licensee.

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

The Manager is required to immediately report to the Licensee any serious cyber safety incident or issue arising from the situations detailed in (e).

Reporting to Licensee

The Manager is required to make regular reports to the Licensee. Included in these reports should be the cyber safety measures that Grow Early Education 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.

Alignment with Other Policies

This policy aligns with the Child Protection Policy, and with Centre Human Resource policies.

Relevant Background (including legislation/regulation references)

Licensing Criteria 2008, Health and Safety, Child Protection:

- HS32: all practicable steps are taken to protect children from exposure to inappropriate material (for example, of an explicitly sexual or violent nature).
- www.netsafe.org.nz.
- The Ministry of Education (MOE) website has information and guidelines in their ICT infrastructure section www.minedu.govt.nz.

Impacts of Policy on Staff, Parents, Children

The use of ICT as part of the centre's activities is essential. It allows staff to research and prepare curriculum-related activities, research and assessment. It can on occasion be used as part of an activity involving (some of) the children, which requires employing safeguarding procedures. Finally, the administration of the centre is dependent upon a number of ICT functions.

The risk of inadvertently accessing inappropriate material via the Internet or from imported material used via the centre's ICT platform of the inappropriate use of that platform is unacceptable and requires constant vigilance by all staff.

Where misuse of the centre's ICT platform occurs, the incident will be investigated by centre management and may result in disciplinary action.

Alignment with the Centre Philosophy

This policy ensures a safe environment, a crucial part of creating and maintaining the well-being of children in our care.

Implementation

Clear procedures have been developed and staff trained to follow them.

Review

Review annually or when there is a significant change in the policy topic.

Authorised:	Jayne Dahlberg
Date:	January 2025
Review Date:	February 2026
Consultation Undertaken:	ECC, Website, Staff Hui, Newsletter