Cybersafety Policy

Purpose

1. Rotorua Girls' High School Childcare Trust acknowledges that:
   a. The Internet and Information Communication Technologies (ICT) play an increasingly important role in the learning of young children, and for centre administration.
   b. The establishment and implementation of a Cybersafety Policy and Cybersafety Use Agreements for teachers and whānau
      i. Contributes to the provision of a positive learning environment as described in the Education (Early Childhood Services) 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
      iii. Assists the centre to meet its obligation 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) 1998

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 the centre to:

a. Meet its legal obligations as outlined in the previous section;
b. Provide guidance to teachers, parents, whānau and visitors regarding the safe and responsible use of ICT at Rotorua Girls' High School Childcare Trust or at any centre related activities;
c. Educate all stakeholders regarding safe and responsible use of ICT;
d. Provide a safe and functional network.

Definitions

The following are definitions of Cybersafety for this 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 desktop and laptop computers, digital cameras, mobile phones, and or other devices deemed to be ICT;
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 trip, centre family function, sporting or cultural event, wherever its location.

Cybersafety Practice at Rotorua Girls' High School Childcare Trust

1. Procedure

The 'Person Responsible' is required to put in place a Cybersafety Programme. This programme should include:

a. This Cybersafety Policy and comprehensive Cybersafety Use Agreement for teachers, parents and whānau, and visitors;
b. Security systems which represent good practice including:
    i. updated anti-virus software;
    ii. updated firewall software or hardware;
    iii. updated anti-spy ware software;
    iv. regularly patched operating system;
    v. appropriate storage of ICT equipment/devices.
c. Cybersafety education for teachers, children, and for the centre's community (e.g. through NetSafe)

2. Permitted Use

Use of the Rotorua Girls' High School Childcare Trust 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. Teachers who have signed the Cybersafety Use Agreement;
b. Parents and whānau of enrolled children, and or other visitors who have signed the Cybersafety Use Agreement;
c. Student teachers who have signed the Cybersafety Use Agreement;
d. Persons contracted to carry out work at the centre *and* at the discretion of the 'Person Responsible'.

3. Privately Owned/Leased ICT Equipment/Devices

Use of privately owned/leased ICT equipment/devices (including mobile phones) at the centre or at any centre related activity is restricted to activities which are appropriate to the centre learning environment, and subject to the centre's Cybersafety Use Agreement. This includes any stored storage of any images or material, or the use of stored images or material, brought toat the centre or any centre-related activity, on any device.

4. Appropriate Use and Content

a. The 'Person Responsible' will provide guidance as to what photographs, video or other digital media usage is considered appropriate to the centre learning environment. (see also guidance provided in the Cybersafety Use Agreement);

b. The ‘Person Responsible’ 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;
c. Parents/whanau and visitors must consult the ‘Person Responsible’ before taking any photographs, video, or making any other recordings using any device while at the centre or any centre-related activity;
d. Parents/whanau or visitors to the Centre may not upload, transmit or in any other way disseminate photographs, video, or any other recordings featuring any child, parent, or visitor at the centre or involved in any centre-related activity without the express consent of those individuals and/or their parents/guardians.

5. User Accounts and Passwords

Access to the centre’s computer network, requires a password protected personal user account. Access to the internet requires a password on all computers, with the exception of white listed websites available to children during supervised access using RGHSCT devices.

6. 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 using the centre’s computers and/or network facilities, either during or outside centre hours.

7. Ownership of Electronic Files or Data

Any electronic data or files created or modified for the purpose of completing work on behalf of the centre on any ICT, regardless of who owns the ICT, are the property of Rotorua Girls’ High School Childcare Trust, unless otherwise agreed.

8. Auditing

a. The Trust Committee may from time to time, at its discretion, conduct an audit of the centre computer network, internet access facilities, computers and other centre ICTequipment/devices;
b. Conducting an audit does not give any representative of Rotorua Girls’ High School Childcare Trust Committee the right to enter the home of teachers, nor the right to seize or search any ICT equipment/devices belonging to that person.

9. Inappropriate Activities/Material

a. The 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 centre network, Internet 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 materials or activities, as defined in the Films, Videos and Publications Classifications Act 1993;
    ii. Save or distribute such material, by coping, storing or printing.
c. In the event of: accidental access to inappropriate material by teachers, parents, whānau, visitors or contractors:
    i. At the lower range of seriousness (e.g. spam): users should delete the material;
    ii. If the nature of such material is somewhat more serious (e.g spam containing inappropriate images, but not illegal images): users should delete the material and also see a member of centre management in order to log the incident in the ICT Incident Log Book.[1] If uncertain as to the seriousness of the incident the material must be removed from view and, the 'Person Responsible' must be consulted. When in doubt, log the incident.
    iii. Where material is clearly of a much more serious nature, or which appears to be illegal, users will:
        a. Remove the material from view (as above) and log it in the ICT incident log book;
        b. Report the incident immediately to the 'Person Responsible' who will take such further action as may be required under this policy.

10. Unauthorised Software or Hardware

Authorisation from the 'Person Responsible' must be gained before any attempts to download, install, connect or utilise any unauthorized software or hardware onto or with any Rotorua Girls' High School Childcare Trust 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 must speak with the 'Person Responsible'.

11. Children's Use of Internet and Email

a. Children will be actively supervised by teachers, or someone who has signed a Rotorua Girls' High School Childcare Trust 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 or post to their online portfolio only under the active supervision of teachers.

[1] The ICT Incident Log Book is to be kept by the 'Person Responsible' next to the main computer.

12. Confidentiality and Privacy

a. 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.
b. The principles of confidentiality and privacy extend to accessing or inadvertently viewing information about personnel, or children and their families, which is stored on any medium or on any device;

Teachers or other employees 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).

13. Cybersafety Training

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

14. Reporting to Board of Trustees

The 'Person Responsible' will make regular reports to the Rotorua Girls High School Childcare Trust Board. These reports shall include, but not be limited to, issues or incidents which have arisen since the previous report and did not require immediate reporting at the time (including and any recommendations), any professional development requirements.

15. Anonymity of children

As part of the cybersafety process, children's e-portfolios will not contain any surnames, addresses or personal phone numbers. RGHSCT will leave profiles of all e-portfolios intentionally blank, and the sites will be closed.

16. Breach

All cases of breach of the RGHSCT Cybersafety Policy will be addressed as deemed appropriate according to, but not limited to, the guidelines outlined below.

a. Staff

i. All cases of breach of the RGHSCT Cybersafety Policy will, in the first instance, be dealt with by the 'Person Responsible';
ii. In cases of breaches of the policy deemed 'serious' by the 'Person Responsible', the RGHSCT Committee Chair shall be notified and involved in determining an appropriate response. Where deemed necessary, the full RGHSCT Committee shall be advised and involved;
iii. In cases of breaches of the policy involving illegality, the 'Person Responsible', in consultation with the RGHSCT Committee Chair, will refer the matter to the police. The full RGHSCT Committee shall be notified;

iv. Consequences for breach will, depending on the level of the breach as outlined above, be at the discretion of the 'Person Responsible', the RGHSCT Chair, and/or the full RGHSCT Committee, and may involve disciplinary action up to, and including, termination of employment.

b. Parents/whanau, visitors to the Centre

i. All cases of breach of the RGHSCT Cybersafety Policy will, in the first instance, be dealt with by the 'Person Responsible';
ii. In cases of breaches of the policy deemed 'serious' by the 'Person Responsible', the RGHSCT Committee Chair shall be notified and involved in determining an appropriate response. Where deemed necessary, the full RGHSCT Committee shall be advised and involved;
iii. In cases of breaches of the policy involving illegality, the 'Person Responsible', in consultation with the RGHSCT Committee Chair, will refer the matter to the police. The full RGHSCT Committee shall be notified;
iv. Consequences for breach will, depending on the level of the breach as outlined above, be at the discretion of the 'Person Responsible', the RGHSCT Chair, and/or the full RGHSCT Committee, and may involve action up to, and including, exclusion of the offending individual/s from the Centre and all Centre-related activities, or the termination of the enrolment of the child/children of the offending individual/s at the RGHSCT.

References

Acts

Films, Videos and Publications Classifications Act 1993
Health and Safety in Employment Act 1992

Regulations

Education (Early Childhood Services) Regulations 2008

Other

Ministry of Education (1998) *Quality in Action Te Mahi Whai Hua*. Wellington: Learning Media.
Ministry of Education Guidelines, Privacy, Safety and Copyright, Ministry of Education, Wellington.

This policy will be reviewed as per the policy review schedule.

Date: 21 October 2019