Greymouth High School Board of Trustees

GREYMOUTH HIGH SCHOOL
Te Kura Tuarua O Mawhera

Digital Safety Policy

Policy Statement

Greymouth High School has a statutory responsibility to maintain a safe physical and emotional environment. We place a high priority on providing the school with Information & Communication Technology (ICT) resources to support student learning. However the School recognises that technologies can also be used inappropriately.

Guidelines

Appropriate use of ICT in the School Environment

1. No staff member or student may use the School internet facilities and ICT resources unless the Responsible Use Agreement has been signed and returned to the school. Signed originals will be kept on staff members' files. The Responsible Use Agreements also apply to the use of privately owned ICT devices on the school site or at any school related activity, regardless of its location. Digital devices related to the Toki Pounamu agreement must also follow the Kawa of Care Cybersafe agreement related to these devices.
2. Use of the internet and School ICT resources by staff, students and other approved users at Greymouth High School is to be limited to educational, professional development, and personal usage appropriate in the school environment.
3. Content expressed on a social networking site (such as Youtube, Twitter, Flickr, Facebook etc) and Short Message Service (SMS), should never cause harm or threaten to be harmful to any one person or group of people. Students should not use a social networking site and SMS's for the purpose of harassing or defaming another member of the School community, or for bringing the name of the School into disrepute.
4. Staff or Students uploading any text or image to a social networking site should consider if they are willing or comfortable to have it displayed in a public forum, such as a student assembly. If not, they should not upload the material.
5. The school deploys filtering systems to restrict access to internet content and services.

Privacy and Copyright

1. Staff and Students need to be mindful of issues relating to confidentiality, such as sighting student or staff information, taking photos and recording sound or video. Verbal consent must be obtained from the student/staff before the image is shared/published in anyway. Collecting data and the secure storage of personal details and information (including images) will be subject to the provisions of the Privacy Act 1993.
2. Students need to be mindful of copyright laws when publishing images or text. Publishing of such material requires proper citation and permission from the author and/or subject.
3. Staff members should not allow any current students access to their personal social networking site. All settings should be set to 'private'. Where social media is used for school purposes, a link must be sent to the Principal for inclusion in our register of staff-student social media links.
4. The School name and logo must not be published on personal networking pages of staff or students.
5. The School believes the privacy of students and staff is paramount and will take appropriate action against individuals who use social networking sites or other ICT resources inappropriately.

Monitoring by the School

1. The School monitors and reviews the activities of all users. This includes personal emails sent and received on the School laptops, computers and/or network facilities at all times.
2. The School has the right to audit material on all School ICT equipment/devices that is owned or leased by the School at any time. The School may also confiscate privately owned ICT equipment/devices used on the School site or at any school related activity if there is reasonable belief of non-compliance with this policy.
3. This policy also applies to visitors, contractors or other personnel in the school or on school-related activities who are using either school devices or network facilities. Anyone unsure about whether it is appropriate to have a particular device at school or at a school-related activity or whether the planned use of a particular device is appropriate, must check with the school.
4. The safety of students is of paramount concern. Any apparent breach of this policy, the school's procedures and The Responsible Use Agreement can undermine the values of the school and the safety of the learning environment and will be taken seriously. The response to individual incidents involving students will follow the system described in the Student Handbook and for staff the relevant Employment Agreement, Staff Code of Conduct and school policies. If illegal or objectionable material or activities are suspected, the matter may need to be reported to the Police in addition to any disciplinary response made by the school as a result of its investigation.

The following terms are used in this policy:

1. The abbreviation "ICT" refers to the term "Information and Communication Technologies".
2. "School ICT" refers to the school's computer network, internet access facilities, computers and other school ICT equipment/devices as outline in (3) below.
3. The term "ICT equipment/devices" used in this document includes but is not limited to, computers (such as desktops, laptops, PDAs/Chromebooks) 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.
4. 'Objectionable' in this policy means material that deals with matters such as sex, cruelty, or violence in such a manner that it is likely to be injurious to the good of students/staff or incompatible with a school environment. This is intended to be inclusive of the definition used in the Films, Videos and Publications Classification Act 1993.

Monitoring of Compliance

The Board will monitor compliance with this policy through:

- The Principal's reports on Digital Safety and any changes to the Responsible Use Agreements
- The Board's own cyclic review of this policy

Signed: ..... **Date:** 6/07/2016

Review Date: 2018