Raumati Beach School

Updated MARCH 2022

Contents

Sections

A) Aim:

To provide internet access and safe protocols for the use of all electronic communications devices/facilities within the school so all staff and students can:

1. Become effective and safe users of the internet.
2. Extend their awareness and knowledge of the internet.
3. Become motivated, responsible, independent users of the internet.
4. Become safe users of cellphones
5. Use email communications safely and effectively

B) On internet use at school:

Use of the internet facilities at this school is provided to support ongoing student/staff learning. This includes personal use and use for professional development of staff. Staff are reminded that they should ensure responsible access at all times. There is an expectation that if staff use the internet for personal access that they will do so reasonably and out of class contact time.

- Training for staff who wish to use these facilities is available through the teacher responsible for eLearning/Information Communications Technology and is **essential** for the safety and protection of staff, students, and equipment. Staff should approach their Team Lead or the Kaitiaki Team for support
- Students may need to be directed to sites on the internet, rather than surfing. Staff should instruct students on how to do this rather than assume they know how. Staff members **must** gain experience using the internet before letting their students use it.

- Teachers supporting BYOD in their classrooms who do not have a locking cupboard can request a locking filing cabinet to store devices in their classrooms. They need to make this request to the Principal.
- It is envisaged that teachers using BYOD will be expected to make full use of Google Apps for Education (GAFE)
- The school has invested in the EDUCA platform as a parent communication tool . ALL Teaching Staff from Year 1 - Year 8 are expected to actively use this tool.
- The teacher in charge of eLearning/ICT will provide training in the use of Google Apps or other key programmes as required.
- Teachers using BYOD will be encouraged to run a Digital Citizenship programme with their students.
- Staff will have individual School email accounts available to them. The agreed email format will be initialandlastname@raumatibeach.school.nz
- Students will have individual school email accounts available to them upon teacher request. The agreed email format will be firstnameandlastinitial@raumatibeach.school.nz
- In consultation with the Principal, staff can request website links be placed on the school web pages (home page for browsers) to provide quick access to particular sites.

C) Student use of the internet:

All students must sign the School Agreement AND have the signed permission of a parent/caregiver before using the school network. These documents will be kept on file in the office and are usually done at the time of enrolment. Class teachers may request to view this file which can be found in the main office. This form is part of the school enrollment information.

- It is advisable that a teacher/adult be in the room, or able to observe students, whenever a student uses the internet. But use of the internet should work on a basis of trust. With the increase of BYOD and more flexible learning environments it is advisable the teacher adopts a “roving,” approach to ensure appropriate use.

- Students should seek permission to use the network outside of normal school hours.

- Students may bring their own devices such as iPads, Netbooks, Chromebooks etc to school.
    - They must seek permission of their teacher to do so.
    - Devices are brought at the students own risk. The school is not responsible for damage that may be caused to these devices. Parents should check that these devices are adequately insured.
    - The school has a right to ask to look at content, which may be stored on their device.
    - If the school suspects there is content which in their view is objectionable, the device will be confiscated and parents will be contacted.
    - Students who bring/share objectionable material will be subject to the school’s disciplinary procedures.
    - The school is part of the Whakaaro Hou Trust. The trust supports students from Year 5 upwards to access Chromebooks for their learning.

- Students may request wireless access.

- It is expected that they will use this for schoolwork or other approved activity.
- This is given to them on trust and will only be the BYOD access.
- If a student is caught downloading material for personal (what could reasonably be termed reasonable and acceptable) use over using the school wireless network, they may be liable for data charges.
- If a student knowingly shares network keys with other students outside of RBS they will be subject to the school's normal disciplinary processes.
- This may also include a period where they will not be able to use the school network without direct supervision.
- If due to this malicious use the school is required to reset network keys the costs associated with this may be passed onto the parent.

Any use of the school network, other than that specified here, e.g. by staff or student's family, or use after hours, must be with the agreement of the Principal/DP or the teacher/s with responsibility for eLearning/I.C.T. All school procedures apply to out of school use.

D) Safety issues:

- Filtering will be used (N4L).
- The school will continue to refine methods of improving safety on the internet.
- Students who produce web pages or posts outside of school regarding other students, staff, or the school which are deemed by the Principal/DP to be offensive will be subject to disciplinary action, which may include stand down or exclusion. Offensive material will be removed immediately. If necessary the school will refer these matters to the police.
- The school has no tolerance towards "cyber bullying." Students involved in this will be subject to the school relationship management procedures. Abusive or threatening digital content (messages, photos, audio or videos) will be reported to the Police. Incidents of cyber bullying by students outside of school should be reported directly to the Police by the parents concerned.
- Digital information recorded at school and posted in an online forum, or shared with others, without the permission of the student/teacher will be subject to the school's relationship management procedures.
- Students who attempt to access objectionable material will be subject to the school's relationship management procedures. Parents will be contacted to discuss the school's concern. It is likely that any attempt to access objectionable material will result in the loss of access and any use of ICT equipment would be limited and monitored for a period of time. Serious breaches would be subject to stand down.

E) Cell Phones / SmartWatches

Cell phones / SmartWatch Technology are both an important communication device and a potential learning tool. The following guidelines apply to the use of cell phones / Smart Watches by students while at school.

- Students are not allowed cell phones / Smart Watches during school hours (unless it is for a structured supervised learning activity). If they bring them to school they must switch them off and hand them into the school office when they arrive.

  They may collect them again at home time. Cell Phones / Smart Watches found in students' possession during the day will be sent to the office or if this is of ongoing concern, will be confiscated and given to the Deputy Principal. They will be held for collection only by the child's parent or caregiver.
- If cellphones are required for a supervised learning activity a process will be in place to allow approved students to collect these at the teacher's request during the day.
- The school cannot take responsibility for content accessed through SIM-enabled phones/smartwatches. If undesirable content is discovered, the student will be dealt with under the school relationship management procedures.

F) Email

Email is a recognized form of communication, especially between parents and staff. The following guidelines apply to email communications.

- It is envisaged that student email communication will be monitored through an online dashboard such as Google Classroom. Teachers will have access to all emails sent, received and trashed. Inappropriate use of the school email system will see students' accounts suspended.
- Parents will only communicate with staff members through their school email school, admin email or an email freely provided by the staff member.
- It is recommended that staff members should only use and provide school email addresses. Parents will be informed as to the protocol staff email addresses follow via the school website.
- Staff are not obliged to reply to any emails that may come through to personal email addresses. All correspondence must come via school addresses.
- Staff are not required to answer emails outside of what might be deemed normal working hours. While this may vary from staff member to staff member it is not expected that a teacher responds in the evening or during the weekend. Staff may choose to do so if they wish, however this is at their own discretion.

- Abusive emails will be notified to the BOT. A formal letter will be written from the Chairperson, to the author of the email stating the BOT's non-tolerance of this behaviour. Failure to comply will lead to the correspondents email address being blocked as will all further electronic communication. The BOT will also refer matters to the Police if necessary. In extreme cases the school (BOT) may seek a restraint order or trespass notice in order to protect staff.

- Threatening emails will be referred straight to the Police. Support will be provided to the staff member who received the email.

Updated: MARCH 2022