Rangiora High School
Board of Trustees

Staff Social Media Procedural Policy

Rationale

We are committed to maintaining the highest standards of professional behaviour, and a work environment which is safe. In their use of social media, **staff employed by Rangiora High School** have extra responsibility in preserving confidentiality, privacy of individuals and maintaining professional standards. The following policy promotes the positive use of social media by staff.

Purpose

Anyone using social media needs to be aware that any information published, including images, becomes public and cannot be controlled; it can be shared, reposted, altered, and exist forever – the Internet never forgets...

Social media includes Facebook, email groups, blogs, Twitter, LinkedIn, and any Internet based site that allows people to connect and share information.

Guidelines

In Professional Role:

Staff may use social media as part of their role at school, for example, in classroom blogs, the school website, and/or Facebook page; and to communicate with members of the school community. The appropriate use of social media at school encourages students to confidently use the technology and understand the issues involved.

Staff should:

Inform parents and caregivers why and how they are using social media in their teaching. Take care to represent the school and its individuals in a respectful and positive way, and in accordance with the School's Privacy Policy.

Teachers should check that the material they are publishing, relating to or linking, is suitable and accurate. Be sure to acknowledge your sources, and conform to any Copyright restrictions.

Texts and emails:

Electronic communication is easy and popular, particularly for broadcasting information about school closures, or school-wide events. For some interactions, a phone call or a face-to face meeting is more appropriate than a text or email.

Also, consider whose responsibility it is to communicate specific information. In the case of a serious incident or crisis, the Principal or a nominated spokesperson may be the only one with authority to pass on information or comment publicly. If you're not sure about passing on information, check!

Media Requests:

If a response to a story is requested by the media in any form, the request from that media outlet should be directed to the Principal in the first instance. Staff are not authorised to speak on behalf of Rangiora High School and should not feel pressured by a media outlet to provide a response.

All staff members are encouraged to be aware of possible news items to further promote the values and purpose of the school. They are also encouraged to identify and notify senior leadership should they become aware of potential negative publicity which may impact on the School or staff/students.

Facebook:

Rangiora High School uses an official Facebook page to promote events and circulate information to the local school and general community. The Facebook page is monitored and maintained by Deputy Principal with responsibility – he is responsible for communicating via the RHS Facebook page, and for the moderation of and response to online comments via Facebook.

The following guidelines are intended for staff who are administering to and communicating via the Facebook page or any other form of media which may become publicly available.

- All content and images must be consistent with RHS' stated values and beliefs or its agreed position on any matter contained therein;
- "The Internet never forgets" – this means everything published will be visible to the world for a very, very long time. If you are about to publish something that makes you even the slightest bit uncomfortable or unsure, review it, seek a colleague's opinion and/or go back to the Principal to discuss;
- "For internal use only" means not for external publication. In no circumstances should staff names, addresses, phone numbers, other details be published via social media;
- All Rangiora HIgh School employees sign a Responsible Use Agreement as part of their Employment Contract on commencement of employment with Rangiora High School;
- Staff are not to comment on legal or other issues via Social Media. Staff are not permitted to make any statements to the press or any other public media via social media on matters relating to the school;

- Staff are to respect their audience at all times. This means no use of ethnic slurs, personal insults, obscenity, or otherwise engaging in any conduct that would not be acceptable in the RHS workplace. You should also show proper consideration for your online recipient's privacy and for topics that may be considered objectionable or inflammatory (such as religion or politics);
- Under no circumstances should Rangiora HIgh School staff publicly endorse any of the following via social media:
    o   a political party or opinion;
    o   a religious entity or opinion;
    o   any other organisation's opinion;
    o   a commercial product or service;
  unless expressly instructed to do so by the Principal or the Board Chairperson;
- In the instance an error or mistake is inadvertently published via Social Media, staff have a responsibility to respond asap with an apology and the correction or, if it is possible to modify an earlier post, do this but make it clear that this modification has been made;
- Staff are required to adhere to Copyright. This means that RHS are not permitted to share or publish via social media another person's or organisation's work, image or logo without their permission.

Using Social Media in your Personal Life

Teachers' personal use of social media must also be governed by confidentiality and professional standards. As well as the general points above, teachers must be aware:

-
- **That they need to regularly check** privacy settings are appropriate **(i.e. the tightest privacy settings possible are set)**, and make sure they understand the terms of service of the social media platforms you use, specifically, how your posts may be accessed, re-used, or republished.
- Maintain a professional boundary. **As no employee may bring Rangiora HIgh School into disrepute on any website.** It is strongly recommended that staff consider
    ○ **Not identifying themselves as being associated with the school by using a separate personal email address including for social media**
    ○ whether it is appropriate to extend or accept friend or connection requests with parents, or others involved with the school.
    ○ **do not accept friend requests from current pupils, or ex-pupils under the age of 20. That the parents are notified if a young person sends a friend request**
    ○ how material or images posted of you reflect on you as a professional associated with the school
    ○ **Not discussing anything to do with school, pupils or other staff members, or posting photos of school events**
    ○ **Do not use social media on school devices, or on personal devices while on the school premises**

Related Policies

- ❏ Creative Commons Procedural Policy
- ❏ Professional Boundaries Policy

Documentation

RHS Staff Handbook
Education Council: Teachers and Social Media

Date of Review	2019
Date of Next Review	2022
Signed by the Board Chair	

Appendix 1: Cybersafety Use Agreement for All School Staff

This document is comprised of this cover page and three sections:
Section A: Important Cyber Safety Initiatives and Rules
Section B: Some Important Staff Obligations Regarding Student Cybersafety
Section C: Staff Cybersafety Use Agreement Form

Instructions for Staff
1. Please read the entire document carefully.
2. If any clarification is required, it should be discussed with the Deputy Principal with responsibility for IT or the Principal before the document is signed. Additional background information on user agreements can be found on the NetSafe website www.netsafe.org.nz/ua
3. Detach Section C, sign and return it to the Principal's PA for filing.
4. It is important to retain the remaining pages for future reference.

Important terms used in this document:
(a) The abbreviation 'ICT' in this document refers to the term 'Information and Communication Technologies'
(b) 'Cybersafety' refers to the safe use of the Internet and ICT equipment/devices, including mobile phones
(c) 'School ICT' refers to the school's computer network, Internet access facilities, computers, and other school ICT equipment/devices as outlined in (d) below
(d) The term 'ICT equipment/devices' used in this document, includes but is not limited to; computers (such as desktops, laptops, PDAs), 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, gaming consoles, video and audio players/receivers (such as portable CD and DVD players), and any other, similar, technologies as they come into use
(e) 'Objectionable' in this agreement 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 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.

Additional information can be found on NetSafe's website
www.netsafe.org.nz/ua

SECTION A

Important Cyber safety Initiatives and Rules

The measures to ensure the cybersafety of Rangiora High School outlined in this document are based on our core values.

The School's computer network, Internet access facilities, computers and other school ICT equipment/devices bring great benefits to the teaching and learning programmes at Rangiora High School, and to the effective operation of the School.

Our school has rigorous cybersafety practices in place, which include cybersafety user agreements for all school staff and students.

The overall goal of the school in this matter is to create and maintain a cybersafety culture which is in keeping with the values of the school, and legislative and professional obligations. This user agreement includes information about your obligations, responsibilities, and the nature of possible consequences associated with cybersafety breaches which undermine the safety of the school environment.

1. Cybersafety User Agreements

    1.1 All staff, students and volunteers, *whether or not* they make use of the school's computer network, Internet access facilities, computers and other ICT equipment/devices in the school environment, will be issued with a user agreement.

    1.2 Staff are required to read these pages carefully, and return the signed use agreement form in Section C to the school office for filing.

    1.3 The school's computer network, Internet access facilities, computers and other school ICT equipment/devices are for educational purposes appropriate to the school environment. Staff may also use school ICT for professional development and personal use which is both reasonable and appropriate to the school environment. This applies whether the ICT equipment is owned or leased either partially or wholly by the school, and used on *or* off the school site.

    1.4 Any staff member who has a signed use agreement with the school and allows another person who does not have a signed use agreement to use the school ICT, is responsible for that use.

2. The use of any privately-owned/leased ICT equipment/devices on the school site, or at any school-related activity must be appropriate to the school environment. This includes any images or material present/stored on privately-owned/leased ICT equipment/devices brought onto the school site, or to any school-related activity. This also includes the use of mobile phones.

3. When using school ICT, or privately-owned ICT on the school site or at any school-related activity, users must not:

    - Initiate access to inappropriate or illegal material
    - Save or distribute such material by copying, storing, printing or showing to other people.

4. Users must not use any electronic communication (e.g. email, text) in a way that could cause offence to others or harass or harm them, put anyone at potential risk, or in any other way be inappropriate to the school environment.

5. Staff are reminded to be aware of professional and ethical obligations when communicating via ICT with students outside school hours.

6. Users must not attempt to download, install or connect any software or hardware onto school ICT equipment, or utilise such software/hardware, unless authorised by the ICT Manager.

7. All material submitted for publication on the school website/intranet(s) should be appropriate to the school environment. Such material can be posted only by those given the authority to do so by senior management.

8. All school ICT equipment/devices should be cared for in a responsible manner. Any damage, loss or theft must be reported immediately to the ICT manager.

9. All users are expected to practise sensible use to limit wastage of computer resources or bandwidth. This includes avoiding unnecessary printing, unnecessary Internet access, uploads or downloads.

10. The users of school ICT equipment and devices must comply with the Copyright Act 1994 and any licensing agreements relating to original work. Users who infringe Copyright may be personally liable under the provisions of the Copyright Act 1994.

11. Passwords must be strong, kept confidential and not shared with anyone else. A strong password is at least 8 characters in length with a mix of lower case (abd . . .) and upper case (ABC . . .) letters, symbols (#*@ . . .) and numerals (123 . . .).

12. Users should not allow any other person access to any equipment/device logged in under their own user account, unless with special permission from senior management.

13. The principles of confidentiality and privacy extend to accessing, inadvertently viewing or disclosing information about staff, or students and their families, stored on the school network or any ICT device. The Ministry of Education guidelines (www.tki.org.nz/r/governance/curriculum/copyguide_e.php) should be followed regarding issues of privacy, safety and copyright associated with student material which staff may wish to publish or post on the school website.

14. Dealing with incidents:

14.1 Any incidents involving the unintentional or deliberate accessing of inappropriate material by staff or students, must be recorded in handwriting in the cybersafety incident book with the date, time and other relevant details.

In the event of access of such material, users should:

1.   Not show others
2.   Close or minimise the window, and
3.
Report the incident as soon as practicable to the cybersafety manager.

14.2 If an incident involves inappropriate material or activities of a serious nature, or is suspected of being illegal, it is necessary for the incident to be reported to the Principal IMMEDIATELY.

15. Any electronic data or files created or modified on behalf of RangioraHigh School on any ICT, regardless of who owns the ICT, are the property of RangioraHigh School.

16. Monitoring by the school:

16.1 The school may monitor traffic and material sent and received using the school's ICT infrastructures.

16.2 The school reserves the right to deploy filtering and/or monitoring software where appropriate to restrict access to certain sites and data, including email.

16.3 Users must not attempt to circumvent filtering or monitoring.

17. Breaches of the agreement:

17.1 A breach of the use agreement may constitute a breach of discipline and may result in a finding of serious misconduct. A serious breach of discipline would include involvement with objectionable material, antisocial activities such as harassment or misuse of the

school ICT in a manner that could be harmful to the safety of the school or call into question the user's suitability to be in a school environment.

17.2   If there is a suspected breach of the use agreement involving privately-owned ICT on the school site or at a school-related activity, the matter may be investigated by the school. The school may request permission to audit that equipment/device(s) as part of its investigation into the alleged incident.

17.3   Involvement with material which is deemed 'objectionable' under the Films, Videos and Publications Classification Act 1993 is serious, and in addition to any inquiry undertaken by the school, the applicable agency involved with investigating offences under the Act may be notified at the commencement, during or after the school's investigation.

18. The school reserves the right to conduct an internal audit of its computer network, Internet access facilities, computers and other school ICT equipment/devices, or commission an independent audit. If deemed necessary, this audit will include any stored content, and all aspects of its use, including email. An audit may include any laptops provided by or subsidised by/through the school or provided/subsidised by the Ministry of Education.

Please note that conducting an audit does not give any representative of Rangiora High School the right to enter the home of school personnel, nor the right to seize or search any ICT equipment/devices belonging to that person, except to the extent permitted by law.

19. Queries or concerns:

19.1   Staff should take any queries or concerns regarding technical matters to the ICT manager.

19.2   Queries or concerns regarding other cybersafety issues should be taken to the Cybersafety Manager, or to the Principal.

19.3   In the event of a serious incident which occurs when the Cybersafety Manager and the Principal are not available, another member of senior management should be informed immediately.

SECTION B
SOME IMPORTANT STAFF REQUIREMENTS REGARDING STUDENT CYBERSAFETY

1. Staff have the professional responsibility to ensure the safety and wellbeing of children using the school's computer network, Internet access facilities, computers and other school ICT equipment/ devices on the school site or at any school-related activity.

2. If staff are aware that a student has not signed a use agreement, the student will not be permitted to use school ICT unless there are special circumstances approved by the principal.

3. If staff are aware of any students who have not signed a use agreement their names should be reported to the Principal, or to the Deputy Principal with Responsibility for IT.

4. Staff should guide students in effective strategies for searching and using the Internet.

5. While students are accessing the Internet in a classroom situation, the supervising staff member should be an active presence. Deputy Principal with Responsibility for IT will advise about Cybersafety protocols regarding Internet access by students in other situations.

6. Staff should support students in following the student use agreement. This includes:

a. Endeavouring to check that all students in their care understand the requirements of the student agreement.

b. Regularly reminding students of the contents of the use agreement they have signed, and encouraging them to make positive use of ICT.

7. Staff are expected to follow the instructions of the Deputy Principal with Responsibility for IT regarding their role in maintaining cybersafety if students of the school are permitted email accounts. (Student email accounts may involve remote access, or access to private non-school email from within the school or on the school network).

Please complete, sign, and date this Staff User Agreement Form which confirms your agreement to follow the obligations and responsibilities outlined in this document. The key obligations and responsibilities are:

- All ICT use must be appropriate to the school environment

- Passwords will be kept confidential

- The principles of confidentiality, privacy and copyright apply.

If you have any queries about the agreement, you are encouraged to discuss them with the Deputy Principal with Responsibility for IT or the Principal before you sign. Once signed, this form should be returned to the Principal's PA for filing with staff records.

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

Additional information can be found on the NetSafe website
www.netsafe.org.nz/ua

Please tick one -

☐ I believe that I have sufficient knowledge to safely supervise the use made by students in my care of the school's computer network, Internet access facilities, computers and other school ICT equipment/devices.

☐ I require additional training/professional development in order to safely supervise the use made by students in my care of the school's computer network, Internet access facilities, computers and other school ICT equipment/ devices.

User Agreement

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 students, the school community and the school environment.

I also understand that breaches of this Staff Cybersafety User Agreement will be investigated and could result in disciplinary action, and where required, referral to law enforcement.

Name: _____

Role in the school: _____

Signature: _____

Date: _____