



## Acceptable Use of Technology and Social Media Policy

### PURPOSE OF THE POLICY

The purpose of this policy is to outline the expectations and standards for student and staff use of laptops, technology and social media. Social media includes any form of online communication or social communications including but not limited to: Facebook, Snapchat, Instagram, YouTube, Twitter, forums, blogs, microblogs, photo sharing, video sharing, Wikis, podcasts, email, chatrooms and discussion boards.

This document also outlines guidelines for the security and confidentiality of electronic information at Rockhampton Girls Grammar School.

### POLICY

Rockhampton Girls Grammar School provides students and staff with technology for educational use. The resources provided include laptops, printers, interactive whiteboards, data projectors, email and internet access.

#### Scope

The policy applies to all staff, students and other users of the school electronic communication facilities and covers the use of school laptops/computers and other electronic devices, including internet access, email protocols, electronic records access and security of information and confidentiality requirements.

#### Responsibility

Principal

#### Point of Contact

IT Manager

### PROCEDURE

Users are granted access to the school's network, internet and email system. ICT usage must comply with the following guidelines.

- **Copyright** - Only software purchased or approved by the school, and installed by the school, can be used on school equipment. It is illegal to copy copyrighted software contrary to the License Agreement; 'pirate' software is not permitted on any school-owned computer.
- **Internet** – Girls Grammar supplies internet access for education-related communication, collaboration and research. Users should be aware that all internet accesses are logged. While on school premises, all internet access must be made through the school network. The use of mobile internet or smart devices to access internet is not permitted. If users are found misusing their access to the internet or email, they will be referred to the Principal and disciplinary action may result.
- **Plagiarism** - Users are expected to respect the privacy and ownership of others' work at all times. This includes not plagiarising information they find on the internet and presenting it as their own work, or copying work of other users, with or without permission.
- **Access** - Computer systems at the school are protected by password access as well as physical barriers where possible. At no time should third parties be given user account details. Laptops issued to users are for the exclusive use of that user. The user should only permit Girls Grammar staff and authorised technician access.
- **Laptop Care and Safety** - School-supplied laptops remain the property of Girls Grammar and must be well-maintained and kept in good working order. They must be carried around school by using the school-provided laptop bag. During school hours, laptops must be secured at all times. This means they should either be in your possession or in a locked locker. Under no circumstances are laptops to be left unattended, in bags, in classrooms, around the school or in unlocked lockers. Laptops are not to be left

at school overnight or over a weekend. Unattended laptops that are found by staff will be taken to IT staff for safe keeping for a period specified by the Principal.

Users are not authorised to change the cosmetic appearance of the laptop in any way – this includes stickers and graffiti on the laptop or laptop case. Intentional damage or marking of the laptop will be rectified at the user’s expense. Any damage must be immediately reported to the IT Department.

- **Insurance** – replacement of misplaced, lost or stolen laptops which were not stored securely is the responsibility of the user and parents will be billed for their replacement. Parents will also be charged for damage to laptops that occurs as a result of laptops being left unattended or unsecured.
- **Data backup** - the school provides a safe and secure platform for the storage of school related documents. This platform is backed up each evening. It is the responsibility of the user to ensure that they are storing their documents in the appropriate location and ensuring that their machine is syncing with the school servers.

While the school makes every effort to keep a backup copy, it is recommended that all secondary students keep a copy of their documents on USB or portable HDD to prevent the loss of important documents in the event an issue occurs. Students are not permitted to save movies / tv shows or music in their documents folder. If these are found to be in a student’s documents folder, the school may delete them.

- **Cyber Bullying** - It is a criminal offence to use laptops, mobile phones or other electronic devices to bully, menace, harass or offend another person. Individuals who use laptops or social media to engage in personal attacks, harass another person, or post private information about another person, take or send photos or objectionable images or bully others, or who use vulgar, derogatory or obscene language, will face disciplinary action. Users found using the school’s system or any non-school electronic device, including mobile phones, for cyber bullying should expect severe disciplinary action, up to and including expulsion, dismissal and/or reporting to the police.
- **Offensive material** - Deliberate attempts to seek, use or transmit material that is illegal, or which would be regarded by reasonable persons as offensive, is not permitted. Should offensive materials be received, they should report them to the IT Department. The Principal has the final say in deciding what is or is not offensive in the school context but will be guided by Section 85ZE of the Commonwealth Crimes Act which states that a person shall not knowingly or recklessly: ‘Use telecommunication services supplied by a carrier in such a way as would be regarded by reasonable persons, as being in all circumstances, offensive.’ Use of the Internet in an offensive manner can result in criminal prosecution.

## AREAS

The following table outlines student responsibilities in relation to technology and social media.

Area	Student responsibilities
<b>Passwords</b>	<ul style="list-style-type: none"> <li>• Keep passwords private and secure. Do not share them with your friends.</li> <li>• Passwords should not be saved on websites, including school-used websites.</li> <li>• Passwords should be changed at least every 90 days to protect personal identity.</li> <li>• The stronger a password is, the harder it is to break. A password should have a minimum of 8 characters:               <ul style="list-style-type: none"> <li>○ upper case letter</li> <li>○ lower case letter</li> <li>○ a number and/or</li> <li>○ a speciality character.</li> </ul> </li> </ul>
<b>Standards</b>	<ul style="list-style-type: none"> <li>• Devices must be fully charged at home and are not to be charged during class without teacher permission.</li> <li>• Whilst on school property, access to the internet is only via the school network. This includes on personal devices.</li> <li>• Personal devices are not to be used during class time, including to contact parents, without permission of teachers.</li> <li>• Students are not to use technology during class time unless directed by a teacher. All use should be for educational purposes and should not impact on learning.</li> </ul>

	<ul style="list-style-type: none"> <li>• Social media should not be used during the school day without the permission of a teacher.</li> </ul>
<b>Mobile Phones</b>	Mobile phones are to be used as per the guidelines published in the Student Planner.
<b>Use of cameras</b>	<ul style="list-style-type: none"> <li>• In-phone cameras are not to be used anywhere where a normal camera would be considered inappropriate e.g. change rooms or toilets.</li> <li>• Students may not take photographs or video of other students on school property or at school events, or in school uniform, without the permission of both the school and the student(s) being photographed/filmed.</li> <li>• Students are not permitted to photograph or video staff without the express permission of the staff member.</li> </ul>
<b>Email</b>	<ul style="list-style-type: none"> <li>• Students are not permitted to access distribution lists or class lists or to send bulk email messages to large numbers of users.</li> <li>• The school's email system must only be used for communication directly linked to a student's education. Students are not permitted to use their school email address for personal correspondence.</li> <li>• Emails sent must represent the school in a positive light and uphold appropriate email etiquette including a salutation, respectful tone and language.</li> <li>• Staff are not required to respond to emails from students outside of normal working hours.</li> </ul>
<b>School reputation</b>	<ul style="list-style-type: none"> <li>• Students may not use the school name, or any images where the school or Girls Grammar students are identifiable, such as students in uniform, without the express permission of the school. This includes but is not limited to posting images or video footage on social media sites.</li> <li>• Student engagement with technology and the use of social media must not impact on the reputation of the school, or any previous/current school staff or any previous/current students.</li> </ul>
<b>Social media</b>	<ul style="list-style-type: none"> <li>• Students are not to send or post messages that contain obscene language, images and/ or threats of violence and/or material that may amount to sexting, pornography, bullying, harassment or stalking or anything of themselves or anyone else in school uniform on any platform.</li> <li>• Students must access their personal profiles only and not log onto the profiles of others, nor must they create false profiles.</li> <li>• Students may only download, or stream via the school network material directly related to their learning during school hours.</li> <li>• Social media access is prohibited during school hours through school carriageways. It is also expected that students would not access social media sites during the school day through other devices unless under teacher direction.</li> <li>• Students should not contact any school staff, either current or former, on personal social media sites.</li> </ul>
<b>School and system security</b>	<ul style="list-style-type: none"> <li>• Students must report inappropriate/unacceptable sites/ material/ documents or viruses immediately to IT staff.</li> <li>• Students must avoid putting the school network at risk by accessing it with a non-school approved device (wireless or internet enabled or software programs e.g. VPNs).</li> <li>• Students must interact with technology and social media on the school network in a lawful way and for educational purposes.</li> <li>• Students may not use their school email address for membership of sites except for educational websites under teacher direction. Students are not permitted to use their school email address for non-school related communications.</li> <li>• Use of technology and social media on the school network may be monitored, logged and checked for appropriateness and the school may remove illegal material from its systems.</li> </ul>
<b>Virus protect and Firewalls</b>	<ul style="list-style-type: none"> <li>• By default, the school activates and locks the firewall "On" on the laptop to protect unwanted access to the laptop. At no time should a user try and turn this feature "OFF".</li> </ul>

	<ul style="list-style-type: none"> <li>• Antivirus is also supplied and maintained by the school. If the laptop gets a virus it is the responsibility of the user to stop using the laptop and to notify the I.T. Department immediately to have the issue rectified.</li> </ul>
<b>Examinations</b>	<ul style="list-style-type: none"> <li>• Students must not bring any unapproved devices, watches, phones or smart gadgets into an examination room. These must be secured in lockers.</li> <li>• If a student brings a device to the examination room, it must be placed on the teacher's desk at the front of the room.</li> </ul>

#### POLICY RELEASE DETAILS

Date of Policy	February 2020
Approved by	Principal
Review Date	Annually
Next Review Date	February 2021
Access	Public Availability – RGGS Website

#### RELATED POLICIES AND DOCUMENTS

Girls Grammar Privacy Policy	Girls Grammar Anti-bullying Policy
Girls Grammar Behaviour Management Policy	Girls Grammar Assessment & Reporting Policy
Girls Grammar Student/Parent & Staff Handbooks	Girls Grammar Electronic Communications Policy
Girls Grammar Information Security Policy	

Name: \_\_\_\_\_ Computer No: \_\_\_\_\_

## Conditions of Supply

In accepting a laptop computer from Girls Grammar, you agree to follow the conditions as set out below. You agree to:

- abide by the Girls Grammar Acceptable Use of Technology and Social Media Policy (AUP).
- care for your laptop.
- store your laptop securely as per the guidelines in the (AUP)
- report any accidental damage or loss.
- accept responsibility for lost laptops.
- accept responsibility for any damage that is not considered normal wear and tear covered by warranty.
- pay for any damage claim lodged for your machine, outside of the first ADP claim each calendar year.
- back up all essential data to the school network at regular intervals as set out in the AUP.
- allow only Girls Grammar approved technicians to carry out maintenance and repair your laptop.

## Privacy Implications

In signing this agreement, you are acknowledging that you understand that the use of the network is monitored and logged and you agree to ensure that:

- the integrity of the network is maintained
- the network is being used for authorised and appropriate activities; and
- you take responsibility for all data you store on the network. Laptops and or other devices attached to the network are considered public. Any such data may be viewed or examined by staff under the direction of the Principal. Information considered private and confidential should not be kept on the Girls Grammar supplied laptop.
- should you wish to install your own legal copies of software (e.g. for conference purposes), you will first discuss your needs with the IT Manager.

## User Declaration

I \_\_\_\_\_ have read and agree to the above agreement.

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

Board of Trustees of Rockhampton Girls Grammar School *trading as*  
Rockhampton Girls Grammar School  
CRICOS Provider No: 00508E