HAMILTON GIRLS' HIGH SCHOOL

Cybersafety Rules

1. Students are required to sign a use agreement before using school Information Communication Technology (ICT) equipment.

2. Use of any Information Communication Technology (ICT) must be appropriate to the school environment.

2.1 For educational purposes only. The school's computer network, Internet access facilities, computers and other school ICT equipment/devices can be used only for educational purposes appropriate to the school environment.

Unacceptable use could include acts of a malicious or nuisance nature, invasion of privacy, harassment, bullying, hacking, taking photos or footage without permission, live streaming, altering the settings on any ICT device or equipment without authorisation,
plagiarism, gaming, impersonation/identity theft, spoofing, gambling, fraud, copyright infringement,
or cheating in an examination. DO NOT USE CHAT ROOMS AT THE SCHOOL OR THE HOSTEL.

2.2 Privately-owned ICT. Use of privately-owned/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/devices brought onto the school site or to any school-related activity (such as, notebooks, mobile phones, USB drives etc).

2.3 Responsibilities regarding access of inappropriate or illegal material. 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 or printing.

In the event of accidental access of such material, users should:
1. not show others
2. close or minimise the window
3. report the incident to a teacher immediately

2.4 Misuse of ICT. ICT must not be used to facilitate behaviour which is either inappropriate in the school environment or illegal, this includes usage at Sonninghill.

3. Individual password logons (user accounts)

3.1 Individual user name and passwords are required and must be kept confidential.

3.2 Access by another person. Users should not allow another person access to any equipment/device logged in under their own user account.

4. Disclosure of personal details

4.1 For personal safety, users should be very careful about revealing personal information about themselves, such as home or email addresses, or any phone numbers including mobile numbers. Nor should such information be passed on about others.

5. Care of ICT equipment

5.1 All school ICT equipment should be cared for in a responsible manner. If ICT equipment is damaged, it may be necessary for the school to inform your parent/legal guardian/caregiver. Your family may have responsibility for the cost of repairs or replacement.

5.2 Any damage, loss or theft must be reported immediately to senior management.

5.3 You should use data storage devices such as USB drives, only in accordance with school regulations.

6. Wastage

6.1 All users are expected to practise sensible use to limit wastage of computer resources or bandwidth. This includes avoiding unnecessary printing, and unnecessary Internet access, uploads or downloads, including photographs and large graphics.

7. Connecting software/hardware

7.1 Users must not attempt to download, install or connect any unauthorised software or hardware onto school ICT equipment, or utilise such software/hardware. This includes wireless technologies.

8. Copyright and licensing

8.1 Copyright laws and licensing agreements must be respected.

9. Posting material

9.1 All material submitted for publication on the school Internet/Intranet should be appropriate to the school environment.

9.2 There is only one official website relating to the school www.hghs.school.nz. Students need permission to contribute material to the school Internet/Intranet site. As well, there should be no student involvement in any unofficial school Internet/Intranet site which purports to be representative of the school or of official school opinion.

10. Monitoring

10.1 The school reserves the right at any time to check emails, work or data on the school's computer network, Internet access facilities, computers and other school ICT equipment.

10.2 If there is a suspected breach of this use agreement, involving privately-owned ICT, the matter may be investigated by the school. The school may ask to check or audit that ICT equipment/device as part of its investigation into the alleged incident.

10.3 The school may use Fotrinet, teaching staff or approved students to monitor students working on the internet.

11. Consequences

11.1 Depending on the seriousness of a particular breach of the use agreement, an appropriate response will be made by the school. Possible responses could include one or more of the following: a discussion with the student, informing parents/legal guardian/ caregiver, loss of student access to school ICT for a period of time, taking disciplinary action. If illegal material or activities are involved, it may be necessary for the school to inform the police.

12. Mobile phones. Cybersafety rules also apply to mobile phones. Mobile phones must not be used for involvement with inappropriate material or activities, such as:

12.1 Upsetting or harassing students, staff and other members of the school community even as a 'joke'.

12.2 Inappropriately using or taking photos or video footage, messages or chatting, web browsing, images or any other functions. Live streaming is unacceptable at school

12.3 Having a mobile phone/device accessible during any assessment.

13. Students need permission from staff to:

13.1 Use storage devices to back-up work or to take work home/back to school. (It is likely the school will need to check any storage device for such things as viruses.)

13.2 Print material when in the classroom situation. Any material printed out of class must be appropriate in the school environment.