Acceptable Student Use of ICT Policy

Policy Statement

This document defines the guidelines and expectations for students' use of ICT resources, which are provided or maintained by the School, including but not limited to hardware, software and network infrastructure.

Rationale

Students are exposed to many dangers when accessing the online environment. All efforts will be made by the School to minimise the exposure to these dangers, but it is not possible to eliminate them all. These dangers may include such things as exposure to physical danger, inappropriate material, unsolicited commercial material, financial risks, harassment and bullying, exploitation, unreliable information, nuisance and sabotage.

Principles

1. Acceptable Use

Students are expected to follow the three principles of acceptable use when using ICT at school.

a. Keep safe

In order to keep safe while using ICT in and outside of school, students have a responsibility to:

- Keep their school-issued unique username and password secure and to disclose it to any other person.
- Keep their school-issued personal storage space on the school's network secure.
- Use their school-issued email address for school and educational purposes only.
- Use the Internet at School for educational purposes only.
- Seek guidance from a staff member before providing personal details online.
- Seek permission from a staff member before posting any personal information or photos on the school network or online.
- Disclose to a staff member any messages they receive that are inappropriate or disturbing.
- Immediately disclose accidental access to inappropriate material to a staff member or main office. This will protect students against an allegation that they have intentionally violated these acceptable use guidelines.
- Notify a staff member if they are offended by another person's use of ICT.
- Notify the main office if they identify a possible security problem.

b. Respect others

Students have a responsibility to:

- Respect all other users of ICT resources at school.
- Respect the privacy of other users.
- Use respectful and kind language communicating with others.
- Follow the same rules and standards online as in real life.
- Follow copyright laws when it comes to movies, music, images and all other online materials.
- Acknowledge the author/owner of the work they have used or quoted.

c. Respect school resources

Students have a responsibility to:

- Only use ICT equipment and resources for educational purposes and under staff supervision.
- Take good care of all ICT equipment and ensure that they use it in a manner that will not damage any devices.
- Only print materials related to their education or as instructed by a staff member.
- Follow staff directions for accessing files, programs, email, Internet resources or any other ICT materials.
- Seek advice from a staff member if unsure of anything relating to ICT.
- Delete all emails from unknown sources that contain attachments.
- Download or send large files (>5 Mb) without staff permission.

Document Name: Acceptable Student Use of ICT Policy_v1.1   Document Location: School/Policies&Procedures
Revision Date: May 2020   Next Review: September May 2022

Page 1 of 3

2. Unacceptable Use

Students are responsible for their actions and activities when using the school network and ICT resources and should not engage in inappropriate or unacceptable use. This includes but may not restricted to the following.

a. Unacceptable practices

Students must not:

- Attempt to change the configuration of any ICT device at school.
- Attempt to gain access to any computer system or service, to which they do not have authorised access. This includes attempting to log in using another person's account or accessing another person's files or emails.
- Make deliberate attempts to disrupt another person's use of ICT.
- Make deliberate attempts to destroy data by hacking, spreading computer viruses or by any other means.
- Engage in any illegal act.
- Install or use software, without the permission of the School.
- Make personal attacks on another person.
- Harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If someone tells a student to stop sending them messages, they must comply with their request.

b. Use of inappropriate language

When using online communication of any kind, users should adhere to traditional communication rules. All other participants should be respected, and appropriate language should be used at all times.

c. Endangering network security

All possible measures are taken to ensure the school network is secure. However, to ensure maximum security students must not:

- Store non-school related materials on the network or any device at school.
- Provide their password or any other personal details to another person under any circumstances.
- Look for network problems or security holes as this will be deemed as an attempt to gain unauthorised access to the network or its resources.
- Post information that can be used to damage or disrupt the network.
- Open emails from unknown sources.
- Open any unknown or unsecure files while using the devices at the School.

d. Accessing inappropriate materials

Access to most inappropriate material has been blocked by the School. However, some materials cannot be filtered, and it is not possible to block all inappropriate material. Students should only attempt to access material when they have been instructed to do so by a staff member. Students must not:

- Access any material unless they have been instructed to do so by a staff member.
- Use ICT devices to access material that:
  - Is profane or obscene (pornography).
  - Advocates illegal acts.
  - Advocates violence or discrimination towards other people.
- Participate in online chats, discussion groups or mailing lists that are not relevant to their education.
- Use school devices to purchase order or sell any goods. If a student needs to purchase something for the School, the relevant staff member must be consulted.

e. Respect for privacy

Students must not:

- Spread a message or materials unless authorised to do so by the owner.
- Take photos, sound or video recordings of people, including background figures and voices, without their explicit permission.

- Record any staff member in or out of class without the prior written permission from that staff member.
- Distribute any private information, pictures or recordings unless they have obtained prior written permission from that person.

f. Cyberbullying

Cyberbullying is the use of technology to bully a person or group with the intent to hurt them socially, psychologically or even physically. It may include cyber harassment, cyberstalking and the invasion of privacy and can occur in many ways, including:

- Abusive texts and emails.
- Hurtful messages, images or videos.
- Imitating others online.
- Excluding others online.
- Humiliating others online.
- Nasty online gossip and chat.

Port School strictly forbids cyberbullying, both on and off campus. It is a breach of the Student Code of Conduct and students engaging in cyberbullying will be subject to disciplinary action, as per the school's Behaviour Management Policy.

3. Consequences of Improper ICT Use

Students are responsible for their actions and activities when using the school network and ICT resources. All student ICT usage violations will be recorded and depending on the severity of the breach the following consequences may apply:

- Loss of access privileges for a period of time.
- School detention or suspension.
- Communication with parents/guardians.
- Potential legal action against illegal activities.

4. Illegal Activities

There are strict laws that govern the use of ICT in Australia. Students need to follow these laws and they may need to speak to the authorities if these laws are broken. All ICT usage at the School is monitored and logged. These logs may be provided to the authorities for any legal investigations.

5. Problem Reporting

Any issues relating to ICT or ICT equipment should be immediately notified to a staff member or the main school office.