Digital Technology and Cybersafety

Digital technology has an increasing role in teaching and learning, in running our workplaces, and in our daily lives. We value our internet facilities and ICT digital technology equipment and the benefits they bring us in learning outcomes and the effective operation of the school. Digital technology equipment includes computers, storage devices, cameras, mobile phones, gaming consoles, video/audio devices, and other digital peripheral devices (including digital watches, smartphones, and tablet computers) whether owned by the school, or privately.

We actively encourage our students to be competent and confident in the use of digital technology; and aware of and able to manage the challenges and issues that go with it. These issues include safety of themselves and others, privacy, copyright, and protection of digital devices and equipment. In short, to be digital citizens. As defined by NetSafe, a digital citizen:

- is a confident and capable user of ICT
- uses technologies to participate in educational, cultural, and economic activities
- uses and develops critical thinking skills in cyberspace
- is literate in the language, symbols, and texts of digital technologies
- is aware of ICT challenges and can manage them effectively
- uses ICT to relate to others in positive, meaningful ways
- demonstrates honesty and integrity and ethical behaviour in their use of digital technology
- respects the concepts of privacy and freedom of speech in a digital world
- contributes and actively promotes the values of digital citizenship.

Below are our procedures to guide our use of the internet, mobile phones, and other digital devices and equipment. We maintain a cybersafe school environment by:

- educating students and the school community about the safe and responsible use of information and communication technologies
- ensuring that systems are effectively maintained, secure, and filtered when necessary
- using NetSafe resources
- allowing for professional development and training for staff
- setting and sharing clear guidelines about acceptable and unacceptable use of the technology, and monitoring these guidelines
- following clear guidelines about **publishing student information** online
- having a clear process for dealing with breaches of the policy or agreements, including any incidents of **cyberbullying**
- following guidelines for the **surrender and retention of digital devices**
- ensuring that all members of the school community understand the policy, and commit to it by signing the appropriate Use Agreement which outlines requirements and expectations
- reviewing use agreements annually.

The policy applies to every member of the school community authorised to use the digital technology equipment, including staff, students, volunteers, trainees, contractors, special visitors, and board members. It applies to digital devices/equipment owned or leased by the school and also those privately owned. It applies whether the digital technology equipment is used at the school, or any other location for a school based activity. This includes off-site access to the school network.

The school maintains the right to monitor, access, and review digital technology use, including email use; and to audit at any time material on the school's equipment. The school may also ask to audit privately owned digital technology devices/equipment used on the school site or at any school related activity.

The school upholds its information privacy principles with the **guidelines** in the Privacy policy.

The safety of students is of paramount concern. Any apparent breach of cybersafety will be taken seriously. The response to individual incidents involving staff will follow the school's procedures which detail how to **Investigate a Formal Complaint or Serious Allegation**. In serious incidents, advice will be sought from an appropriate source, such as NetSafe, the New Zealand School Trustees Association and/or a lawyer with specialist knowledge in this area. There will be special attention paid to the need for specific procedures regarding the gathering of evidence in potentially serious cases. If illegal material or activities are suspected, the matter may need to be reported to the relevant law enforcement agency.

Resources

- TKI: **Digital Citizenship and Cybersafety in Schools**
- **NetSafe**