

Rationale:

Botany Downs Secondary College is committed to creating a safe online learning and working environment and to the development of our students and staff into capable digital citizens. The Board recognises that its obligations under the National Administration Guidelines (NAG 5) extend to the use of the internet and related technologies.

Technology provides significant benefits to learning and school operations. The School Board considers the benefits and risks associated with technology use when making any decisions related to the purchase or use of technology.

Botany Downs Secondary College seeks to foster a culture of successful digital citizenship in our students, staff, and our wider community. We encourage everyone to take responsibility for themselves and others in their use of digital technology and online environments.

The school network and the internet are tools that provide opportunities for valuable and unique learning and teaching experiences. Our goal is to ensure successful and responsible use for all users.

Purpose:

1. To develop and maintain procedures around the safe and responsible use of digital technologies, the school's network and systems, and the internet.
2. To make teaching and learning resources, materials, and software easily accessible and address the need of users to receive and participate in education opportunities around the safe and responsible use of digital technologies and online environments.
3. To ensure the 'safe' use of the internet and network with rigorous CyberSafety practices in place, and relevant training.

Areas of Responsibilities:**Staff:**

- All network activity (including internet and email) should be appropriate to teaching, learning and operational activities.
- Teachers to monitor student use of network in classes and to report misuse or suspected misuse to a member of the Senior Leadership Team.
- To promote privacy and security for other users.
- To protect personal and proprietary data through:
 - Checking suspicious email requests for sensitive information.
 - Reviewing hyperlinks before clicking.
 - Using multistep verification logins.
 - Password management.
 - Locking screens when away from devices.
 - Backup management.
 - Archiving important files in secure locations provided on the network.
 - Seeking written permission to access the network when travelling overseas from the Principal or Business Manager.
- Staff may use the college ICT for personal use which is both reasonable and appropriate to the college environment. This applies whether the ICT equipment is owned or leased either partially or wholly by the college and used on or off the college site. The amount of time spent on non-work-related usage should be reasonable and not interfere with normal work duties.

- The use of any private ICT on the college site, or at any college related activity is subject to the CyberSafety agreement and must be appropriate to the college environment. This includes any images or material present or stored on private ICT equipment brought onto the college site, or to any college related activity.


Network Manager:

- To provide training and support in the use of the network to enable effective and appropriate teaching and learning activity.
- To ensure all users agree to guidelines for use of Network.
- Where necessary and appropriate, monitor network use including Internet sites visited and e-mail sent and received for the purpose of safeguarding staff, students, and the school.
- To examine, amend and delete any inappropriate material as required and to refer inappropriate use and material to appropriate person.
- To protect against any activity that threatens the integrity and efficient operation of the school network.
- To ensure privacy and security.
- To provide the school the assurance of ongoing support and maintenance, and for the recovery of the network in the event of an outage.
- Manage the designated onsite technicians who support the daily needs of the end users in a timely and professional manner.
- To ensure that the network is geographically locked down to New Zealand only.

Other Relevant Documentation/Resources:

- CyberSafety Agreement.
- Netsafe <https://netsafe.org.nz/>.
- New Era Platinum Agreement.
- Ministry of Education Digital Technology Safe and Responsible Use in Schools.

Review Schedule:	Triennially
Review Date:	1 May 2023

Presiding Member Signature:	
Date:	1 May 2023