Hauraki Primary School
Policy Document

Computer Security and Cyber Security

Rationale

Hauraki school students and staff will be responsible, ethical, and productive users of Information and Communication Technologies (ICT) in the school and in society in accordance with the values of Hauraki school, and the principles and values in the New Zealand curriculum.

Purpose

The Hauraki School Board (the Board) is responsible for ensuring the school maintains robust computer security and cyber security practices. We aim to safeguard the school's digital infrastructure, data, and devices through the implementation of layered protections and professional support, including third-party contractors. These safeguards include:

- Appropriate insurance coverage for physical loss or damage of school-owned digital devices and infrastructure.
- Firewall, endpoint protection, and antivirus software to prevent unauthorized access and malicious attacks.
- Timely updates and patch management for operating systems, software, and firmware on all school-owned devices.
- School-installed programs and applications may only be altered or updated with authorisation from designated ICT personnel or the principal.
- Secure, Ministry of Education (the Ministry) approved internet service provider (ISP) and web filtering systems to monitor and protect internet access.
- regular review and risk assessment of digital systems and infrastructure in alignment with Ministry standards and emerging threats.

Guidelines

Access Control

1. All school-owned digital devices and user accounts must be password protected with strong, regularly updated credentials.

2. Staff and students using personal devices on the school network or for school-related purposes are strongly advised to use password protection and ensure their devices meet minimum security requirements.

3. Remote access to the school network must only be made over secure, encrypted Wi-Fi networks (e.g. WPA3 or VPN-protected connections).

4. Where possible, multi-factor authentication (MFA) should be used for accessing sensitive school systems.

Data Protection

5. School information is backed up regularly, either on-site or to a secure cloud environment, in accordance with data retention policies.

6. The school conducts regular audits and reviews of what personal or identifiable information is made publicly available, especially via its website and newsletters.

7. Disposal of confidential or sensitive digital data follows secure erasure procedures or is managed through certified e-waste disposal providers, in accordance with the school's Privacy policy.

8. Staff and students are educated and encouraged to remain vigilant for digital threats including viruses, ransomware, phishing emails, and scams.

9. Staff are expected to report any suspected data breach or cyber incident immediately to the principal or designated IT support person.

Incident Response

10. In the event of a cyber-attack, data breach, or digital security incident, the school will:

    - Immediately isolate affected systems where possible to limit spread.
    - Notify and seek guidance from CERT NZ (Computer Emergency Response Team of New Zealand) and NETSAFE as appropriate.
    - Conduct a post-incident review to determine root cause and adjust security practices accordingly.
    - Inform affected parties where required under privacy regulations.

Internet and Network Infrastructure

11. In accordance with Ministry policy, the school maintains its ICT network to current Ministry standards using approved contractors.

12. The School Property Plan (10YPP) includes a dedicated budget for ICT network maintenance, upgrades, and cybersecurity tools.

13. The school uses network segmentation, secure wireless protocols, and monitoring systems to protect infrastructure and user data.

Signed: Reeber **Date:** 16/6/2025

Presiding Member of the Board **Review Date:** June 2028

Related policies

- Crisis Management
- Health and Safety
- Privacy
- Teacher Laptop Usage