Hauraki Primary School

Policy Document

Computer Security and Cybersecurity

Rationale:

The principal and board are responsible for the school's computer security and cybersecurity and review this regularly.

Purposes:

We have appropriate protections, including the use of third party contractors, to provide protection for the school network and school owned devices, such as:

1. Appropriate insurance for physical loss or damage
2. Firewall and antivirus software
3. Regular updates for operating systems and programs on school devices
4. School installed software programs can only altered under the authorisation of the school
5. A secure internet service provider

Guidelines:

Access control

1. Password protection is used on all school devices and user accounts.
2. We recommend that personal devices used on the school network or containing school information are also password protected.
3. We recommend that remote access to the school network should only be made over secure wifi networks.

Data protection

1. We back up school information as appropriate.
2. The school reviews and considers what personal information is available publicly.
3. Appropriate methods are used for the disposal of Confidential waste in line with Hauraki school's Privacy Policy.
4. Staff and students are encouraged to keep alert for viruses, malware and phishing scams.

If Hauraki Primary School experiences a cyberattack, we contact CERT NZ (New Zealand's Computer Emergency Response Team) for advice and support, as appropriate.

Internet/Network infrastructure

The Ministry of Education requires Hauraki Primary School to keep the school's ICT network maintained to the current Ministry Standard, and uses Ministry-approved contractors for any maintenance or repair work.

Our school property plan contains a budget for maintaining the digital network.

Signed: _____ **Date:** 22/2/22

Presiding Member of the Board **Review Date:** Term 1 2025