Policy: Cyber Safety

Policy Statement

The Jireh Christian School ("the School") Board recognises its responsibility to provide and maintain a safe environment for students and all employees whilst maximising the educational benefits of communication technologies and minimising the risks. Use of the Internet and other communication technologies at the School is to be limited to educational and personal usage appropriate in the School environment. Students will develop the skills, knowledge, attitudes and values to make safe and informed choices while using devices and online spaces through meaningful, authentic learning opportunities.

The communication technologies at the School are available to staff and students under the conditions outlined in their Safe Use Agreement (staff) and Digital Citizenship and Responsible Use Student Agreement (students).

Procedural Guidelines

1. All students must sign the School's Digital Citizenship and Responsible Use Student Agreement outlining the regulations and conditions under which computers and communication technologies may be used while at School. The agreement must also be signed by a parent/caregiver.
2. Students will be supervised while using School facilities, the degree and type of that supervision may vary depending on the type of technology concerned, where the equipment is situated and whether or not the activity is occurring in the classroom.
3. All staff must sign a Safe Use Agreement which includes details of their professional responsibilities and the limits to their own use of the Internet.
4. Educational material on cyber safety will be provided by management to staff and students and to parents/caregivers. Additional safety education will be delivered, where relevant, through teaching programmes and the Jireh Christian School Digital Technologies curriculum.
5. Basic training for staff will be made available by Management, as will appropriate professional development.
6. The necessary filters will be put into place by the School to address cyber safety issues in all venues where the internet and other communication technologies are accessed by staff or students on site.
7. The School will provide an effective electronic security system and will continue to refine methods to improve cyber safety.
8. The Principal will be responsible for the establishment and maintenance of a cyber safety programme in the School. This responsibility may be delegated to the leader of e-learning.
9. The Board supports the right of the School to check communication technology-related work or data of staff or students at any time, and to carry out a comprehensive investigation of any breaches (actual or suspected) of the School's Cyber Safety Policy. Such breaches will be taken seriously and be dealt with through the School's disciplinary and support systems. If illegal material or activities are evidenced, the matter will be reported to the NZ Police or the Department of Internal Affairs Censorship Compliance.

Legislative Compliance:

Harmful Digital Communications Act (2015)
Privacy Act (2020)

Review schedule: Triennially

ADOPTED BY BOARD

Date 12th September 2017 Chairperson **R Thornton (Acting)**

Reviewed Date	14th November 2017	Chairperson **R Thornton**
Reviewed Date	23rd June 2020	Chairperson **M Causley**
Reviewed Date	26th March 2024	Presiding Member **A Coombridge**