NAG 5.2

Policy: School Cyber Safety

Policy Statement

The Jireh Christian School Board of Trustees 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 Jireh Christian School is to be limited to educational and personal usage appropriate in the School environment. The digital technologies at Jireh Christian 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

- All students must sign Jireh Christian School's Digital Citizenship and Responsible Use Student Agreement outlining the regulations and conditions under which computers and digital technologies may be used while at school. The agreement must also be signed by a parent/caregiver.
- Students will be supervised while using school facilities; the degree and type of that supervision may vary, dependent on the type of technology concerned, where the equipment is situated and whether or not the activity is occurring in the classroom.
- 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.
- 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.
- Basic training for staff will be made available by Management, as will appropriate professional development.
- The necessary procedures 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.
- The school will provide an effective electronic security system, and will continue to refine methods to improve cyber safety.
- The Principal will be responsible for the establishment and maintenance of a cyber safety programme in the school. This responsibility may be delegated to a member of the Senior Leadership Team.

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 suspected, the matter will be reported to the Police or the Department of Internal Affairs Censorship Compliance. Staff will be involved in a random IT equipment audit. Staff network passwords will be changed on a regular basis.

Review schedule: Triennially

ADOPTED BY BOARD OF TRUSTEES

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

Reviewed Date 14th November 2017 Chairperson **R Thornton**