

## Policy: **School Cyber Safety**

---

### **Policy Statement**

The Manurewa High 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 Manurewa High School is to be limited to educational and personal usage appropriate in the School environment.

The communication technologies at Manurewa High School are available to staff and students under the conditions outlined in their "Safe Use Agreements".

Appropriate cyber safety measures will be put in place and enforced by the school and action will be taken if these safety regulations are breached by students or staff.

The Cyber Safety Policy applies to all employees of the Board (ie, teaching, support and ancillary staff), students, teacher and other professional trainees assigned to the School from time to time, relief teachers.

### **Procedural Guidelines**

- All students must sign Manurewa High School Computing/Cyber Safety Use 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.
- 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 Cyber Safety 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.

*cont.....*

*Page 2 - School Cyber Safety Policy cont.*

- 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 (see separate Policy).
- Staff network passwords will be changed on a regular basis.

Review schedule: May 2020

<b>ADOPTED BY BOARD OF TRUSTEES</b>			
Date	<b>23 November 2005</b>	Chairperson	<b>S Smith</b>

<b>AMENDED</b>	Date	<b>30 October 2008</b>	Chairperson	<b>S Smith</b>
<b>REVIEWED</b>	Date	<b>26 September 2011</b>	Chairperson	<b>S Smith</b>
<b>REVIEWED/AMENDED</b>	Date	<b>29 May 2017</b>	Chairperson	<b>S Smith</b>
<b>REVIEWED/AMENDED</b>	Date	.....	Chairperson	.....
<b>REVIEWED/AMENDED</b>	Date	.....	Chairperson	.....
<b>REVIEWED/AMENDED</b>	Date	.....	Chairperson	.....