# Safe and Responsible Use of Digital Technology

Refer to Operational Policy 1: Curriculum Delivery, Operational Policy 8: Health and Safety, & Operational Policy 9: Child Protection

**Reviewed:** 15.02.22 **Due for Review:** February 2023

## Purpose:

These procedures are designed to meet the school's statutory obligations to maintain a safe learning environment and to consult with the community on the safe and responsible use of digital technology. The overall goal is to maximise the educational benefits of digital technologies while minimising the risks.

Use of digital technologies at Spotswood Primary School is to be limited to educational and personal usage appropriate in the school environment. Appropriate use also includes staff professional development.

'Other digital technologies' include the mobile phone and technologies associated with internet use e.g. digital camera and webcam. Included, too, are similar technologies still being developed.

Digital technologies at Spotswood Primary School are available to staff and students under certain conditions, as outlined in their signed Use Agreements. The school will make basic training available for staff using these technologies. Associated professional development needs will be considered.

Appropriate cyber safety measures will be put in place and enforced by the school. In order to ensure the safety of the school learning environment, action should be taken if these safety regulations are breached by students or staff.

These procedures apply to all employees of the Board (i.e. teaching, support and ancillary staff) and to all students. It also applies to teachers and other professional trainees assigned to the school from time to time, relief teachers and students.

## Guidelines:

- All students must read or have explained, a Safe and Responsible Use of Digital Technology Agreement outlining the regulations and conditions under which computers and communication technologies may be used while at school or in any way which affects the safety of the school learning environment. A confirmation that this will be discussed with their child (Consent Form Parent/Caregiver) must also be signed when a student is enrolled.

- 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 physically situated and whether or not the activity is occurring in the classroom. ie. restricted and supervised use of Youtube and devices not used by students during break times.

- All staff must meet their obligations in the Staff Code of Conduct. Pages 7 and 8, in particular, outline expectations around the safe and responsible use of digital technology.

- All staff must sign a Laptop Use Agreement and, if they are issued with one, an iPad Use Agreement. These include details of their professional responsibilities and the limits to their own use of the Internet.

- Educational material on cybersafety will be provided by management to staff and students, and to parents/caregivers. As well, additional safety education will be delivered, where relevant, through teaching programmes.

- Basic training for staff in the use of digital technology will be made available by management, as will appropriate professional development.

- The school will provide an effective electronic security system, which is financially practicable. The school will continue to refine methods to improve cybersafety.

- The Principal will be responsible for the establishment and maintenance of a cybersafety programme in the school - the Principal may delegate that responsibility to a member of the Senior Management 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 of the school's cybersafety policies and procedures. Such breaches will be taken seriously and be dealt with through the school's disciplinary and support systems. In such incidents, there will be special attention paid to the need for specific procedures as regards the gathering of evidence. If illegal material or activities are suspected, the matter will be reported to the Police or the Department of Internal Affairs Censorship Compliance.

- The Principal will ensure that school insurance policies include protection against cyber-crime.

- The school will consult with the wider school community and provide opportunities to learn about cybersafety issues.

- Staff are responsible for backing-up files from their laptop or desktop hard-drives on the server and external hard-drives. Server files are backed-up through Smart-Net, a web-based service. However, many school documents are on Google-drive that do not require backing-up.

- Files that may become corrupted or lost may be retrieved through Smart-Net. The Principal and Office Manager are able to request back-up files from Smart-Net.

- The school wifi code will be kept secure. A guest wifi code will be issued to visitors at the discretion of the senior leadership team.

- Staff are expected to keep their passwords secure and update them regularly.

- The Administration Manager will keep a file of staff gmail accounts, server usernames and passwords, and website registration usernames and passwords.

- Teacher laptops and teacher iPads will be password protected to avoid unauthorised users accessing files.

- A team of teachers will be responsible for the overview of computer/device use and maintenance within the school. The team consists of teachers who have a Salary Unit responsibility for Digital Technology.

- Technical assistance for the maintenance and repair of hardware and network systems will

be provided by professional support personnel.

- Technical assistance on the protection and management of files will also be sought by professional personnel.

- Professional advice will be sought to upgrade hardware, software, and systems within the school to meet the needs of the programme.

- All classes will be expected to undertake periods of instruction in-class on available devices where students create and collaborate.

- No out-of-school groups will be permitted to use the computers in the school unless at least two weeks prior arrangement in writing has been made and the permission of the Principal and Teacher in charge of ICT is obtained. The Cybersafety Agreement must be signed by users.

- Staff will use laptop computers for planning, assessment and reporting and can be included in classroom learning programmes.

- Planning for teaching and learning will be done using Google so that it can be readily shared.

For more information please refer to Digital Technology Safe and responsible use in school Ministry of Education 2015.