Cyber Safety Policy

Purpose

Students are exposed to a wide range of connected electronic devices such as laptops, tablets and smartphones. These devices are recognised as beneficial educational tools. However, some students are spending large amounts of time using electronic devices.

There are a number of safety issues on the internet, which pose threats to students' emotional lives and thus their academic lives. Some students are involved in cyber bullying either as perpetrators or as victims. Some students are unaware of safety issues surrounding their digital footprint and are could be at risk of a range of possible problems such as identity theft and sexual predators

Scope

To meet the changing nature of technology and to ensure that students, parents and workers are aware of the risks attached to overuse and unsafe use of the internet. To ensure that all users of Technology at St Paul's School are able to make educated choices regarding these risks.

Cyber safety is the safe responsible and discerning use of Information and Communication Technologies (ICT).

Objective

> To implement and maintain a whole school approach to address the problem of cyber safety.
> To make students aware of the safety issues regarding the internet, gaming, social networking.
> To inform students about the negative consequences that can result from the misuse of the internet.
> To empower students to take ownership of and responsibility for their usage and habits.
> To educate teachers about their role in ensuring that students are using the internet responsibly and safely.
> To support parents in their efforts to ensure that their child are using the internet responsibly and safely.
> To identify those at most risk and provide them with specific support from a range of support mechanisms.

Outcomes

> Workers, students and parents to adhere to the Schools policies and procedures.
> Provide students with relevant skills and strategies to use computers effectively and with a high level of digital literacy.
> Equip students with relevant skills and strategies to manage computer overuse and/or addiction.
> Educate students about cyberbullying and other unacceptable behaviours.
> Educating students about risks concerning internet use and online privacy (release of personal details; photos; sexual predators etc).
> Provide students with effective strategies to protect their digital identity.
> Promote responsible/appropriate digital etiquette.
> Staff to be proactive in enforcing appropriate computer use in classroom.
> Staff to recognise that all incidents of bullying are unacceptable and to be proactive in addressing their issue.

Workers

> To ensure ongoing communication between workers, parents, students and relevant agencies is open and productive.
> To produce and keep updated material to distribute to parents.
> To regularly engage in monitoring activities to gauge the severity of the problems and to set targets for improvement.
> To develop and regularly update an education program as part of the RAVE program and also within curriculum delivery.
> To determine what strategies can assist employees and to use Professional Development Days to disseminate this.
> To ensure that parents and students with concerns are given appropriate support.

Students

> All students will be made aware of the School rules and expectations regarding computer usage and cyber safety.
> All students will develop an understanding that there are rights/ responsibilities, which accompany the correct use of the internet and consequences, which accompany the misuse of the internet.
> Students and their parents will verify their understanding and abide by the Responsible Use Agreement

Parents

> Work in partnership with the School.
> Supervise and manage the students use of technology out of hours and at home.
> Respond to misuse occurring, assisted by the School as appropriate.

Dr Paul Browning
Headmaster
October 2017

Control No.: POL-046   Printed copies of this document are uncontrolled   Page 1 of 1
Version: 1.0   Effective Date: 17/10/2017
Department: Risk and Compliance   Next Review: 17/10/2019