The Education School

CYBERSAFETY POLICY

RATIONALE

The Education School has an obligation to maintain a safe physical and emotional environment for staff and students. This responsibility is increasingly being linked to the use of the Internet and Information, Communication and Learning Technologies (ICLT), and a number of related Cybersafety issues. The Internet and ICLT devices/equipment bring great benefits to the teaching and learning programs, and to the effective operation of the school.

The Education School places a high priority on providing Internet facilities and ICLT devices/equipment which will benefit student learning outcomes and the effective operation of the school. However, it recognises that the presence in the learning environment of these technologies (some provided partly or wholly by the school and some privately owned by staff, students and other members of the school community), can also facilitate anti-social, inappropriate, and even illegal behaviour and activities. The School aims, therefore, to maximise the benefits of these technologies, while at the same time to minimise the dangers and manage the risks.

In order for this policy to be accepted and embraced by The Education School community, it is imperative that all members of the school community provide input into its development. The Education School Cybersafety Committee will be formed and they will be responsible for the establishment of this policy. This committee will comprise staff, students and parents and will ensue that an equal voice is heard

UNDERLYING PRINCIPLES

The policy is written in light of the Mission Statement of the School, whereby the School

.....insert principles of Mission Statement here.....

POLICY

The Education School will develop and maintain rigorous and effective Cybersafety practices which aim to maximise the benefits of the Internet and ICLT devices/equipment to student learning and to the effective operation of the school, whilst minimising and managing any risks.

These Cybersafety practices will aim to not only maintain a cyber safe school environment but also to address the need of students, staff and other members of the school community to receive education about the safe and responsible use of present and developing information and communication technologies.

Associated issues the School will address include the need for relevant education about Cybersafety for the school community, the need for ongoing funding for Cybersafety practices through inclusion in the annual budget, implications for the design and delivery of the curriculum, the deployment of staff, professional development and training, disciplinary responses appropriate to breaches of Cybersafety, the availability of appropriate pastoral support, and potential employment issues. Cybersafety will become a key component of the curriculum at *The Education School* and lessons will be delivered at each Year Level, incorporated into the [insert Learning Area] curriculum.

(Example used to explain curriculum)

In Term 1, Year 7 English students will read and discuss the novel, 'Destroying Avalon' by Kate McCaffrey as an introduction to the topic of Cybersafety. Teachers will be provided with the opportunity to participate in Professional Development Session to improve their knowledge and understanding of the issues and all Cybersafety initiatives will include the opportunity for parental education. Teaching resources will be provided to ensure that teachers have access to current and appropriate curriculum materials. All teachers however have a responsibility to ensure safe online practices within their class and take every opportunity to engage students in relevant dialogue about current Cybersafety issues.

The *Education School* takes seriously its responsibility in providing robust policy, guidelines and education for students in relation to what is deemed acceptable and appropriate online behaviours. The school name, motto, crest, logo and/or uniform must not be used in any way which would result in a negative impact for the school and its community. Students must not post photos of either themselves and/or other students which clearly identity them as a member of the *The Education* School community, nor post photos taken during any school sanctioned activity.

This includes off campus events such as sports days and camps. Students and/or parents must not take photographs or otherwise record members of the school community (other than themselves or their own child) whether intentionally or inadvertently and/or post to the Internet, publish or share without the written permission of the person photographed. (See Photography Policy for more information) School staff, including teaching and non-teaching staff will be provided with clear guidance around the use of personal devices within the wider school setting to ensure the privacy of a student maintained.

No member of the school community will establish or maintain a social networking site which uses the school name, crest, logo or any other name by which the school and its community may be known without the express permission of the Principal or his/her delegate. This includes class based Facebook pages. Members of the school community also have a responsibility to ensure that all online communications are in keeping with the schools expectations in relation to appropriate and respectful interactions with teaching and non-teaching staff. Any form of online abuse will not be tolerated and if occurring, legal advice will be sought to protect the school or person so named.

Students will not post inappropriate comments about individual staff members which if said in person would result in disciplinary action being taken.

Neither the School's network nor the broader Internet [whether accessed on campus or off campus, either during or after school hours, via any application] may be used for any purpose other than that which it was designed. Cyberbullying, harassment, taking, sending and receiving naked or sexually explicit images,(sexting) and other misuses of technology in cyberspace are unacceptable.

"Cyberbullying is a way of delivering covert psychological bullying. It uses information and communication technologies to support deliberate, repeated and hostile behaviour, by an individual or group that is intended to harm others." (Belsey 2007)

Cyberbullying includes, but is not limited to, the following misuses of technology: harassing, teasing, intimidating, threatening, another person by sending or posting inappropriate and hurtful e-mail messages, instant messages, text messages, phone messages, digital pictures or images, or Web site postings (including blogs). One isolated nasty, disrespectful or hurtful comment or post will be a clear breach of school rules, however it will not be categorized as cyberbullying.

The forwarding of private emails, messages, pictures or videos or otherwise inappropriately communicating personal or private information belonging to another person or logging on and pretending to be someone else as well as sending sexually explicit images ('sexting'), intentionally excluding others from an online group and 'liking' or 'sharing' a bullying comment will all be considered as cyberbullying and if this occurs either during school time or after school hours, will constitute a breach of school policy and as such a student will be subject to disciplinary action.

Students must be aware that in certain circumstances where a crime has been committed, they may also be subjected to a criminal investigation by Police over which the school will have no control.

Students who feel that they have been the victims of such misuses of technology should save and store the offending material on their computer, mobile phone or other device. They should then print a copy of the material and immediately report the incident to a teacher. Staff who may have been cyberbullied or threatened online should immediately report such incidences to a member of the School Leadership Team.

All reports of cyberbullying and other technology misuses will be investigated fully and may result in a notification to Police or other authority where the school is legally obliged to do so. Sanctions may include, but are not limited to, the loss of computer privileges, detention, suspension, or expulsion from the School.

This policy and procedures is to be read in conjunction with the School's *Whole School Behaviour, Safe School, Computer Use* and *Electronic Communication* policies and procedures*. [or those relevant policy documents for your school].*

DURATION

This policy will be reviewed every 12 months.

Sample Policy Template prepared by:-

Susan McLean

www.cybersafetysolutions.com.au

Important terms used in this document:

*(a) The abbreviation **'ICLT'** in this document refers to the term 'Information, Communication and Learning Technologies.*

*(b) **'Cybersafety'** refers to the safe and responsible use of the Internet and ICLT equipment/devices, including mobile phones*

*(c) **'School ICLT'** refers to the school's computer network, Internet access facilities, computers, and other school ICLT equipment/devices as outlined in (d) below*

*(d) The term **'ICLT equipment/devices'** used in this document, includes but is not limited to, computers (desktops, laptops and Tablets), storage devices (such as USB and external hard drives), cameras (such as video, digital, webcams), all types of mobile phones, smart TV's Connected watches, Gaming Consoles, and any other, similar, technologies as they come into use.*

**********PLEASE NOTE**********

This Policy document is not intended to be used in its current state. It is provided as a guide to assist schools in the development of their individual Cybersafety policy. It includes a range of options and issues that must be considered in the writing of a Cybersafety policy. A key component of the success or otherwise of any Cybersafety policy will rest with those tasked with the responsibility of writing the policy. It MUST include input from the student body. Its' success will also be linked to the implementation of the Policy, as a policy document alone does not abrogate responsibility to actively educate, manage and resolve online issues that a school is informed about.

A Cybersafety policy for a Primary School or a P – 12 School will vary only in the composition of the document. The key issues to be address will remain the same; however language and other cosmetic changes will occur.