



CYBERSAFETY POLICY

Definition:

Cybersafety is made up of two strands: Cyberbullying and Communicating Safely.

Cyberbullying involves the use of information and communication technologies to support deliberate, repeated, and hostile behaviour by an individual or group that is intended to harm others. Bullies deliberately set out to intimidate, exclude, threaten and/or hurt others repeatedly. Bullying is a clear form of harassment. People who use the internet, email, intranets, phones or similar technologies to bully others are cyberbullies and are breaking the law.

Communicating Safely reflects the need for students to remain safe while using online resources such as social networking tools, like Facebook and MSN messenger, as well as using websites and online resources responsibly and respectfully.

Rationale:

- Bullying in any form is unacceptable. Bullying that is carried out through an internet service, such as email, chat room, discussion group or instant messaging, or through mobile phone technologies such as short messaging service (SMS), is cyberbullying. Cyberbullying will not be tolerated at any level, and consequences exist for students who choose to bully others.
- When speaking, posting content or meeting people online, internet users need to be aware that there are some risks, including inappropriate contact with other people. An understanding of these risks should reduce the dangers to our students.

Aims:

- To educate students on their role and responsibilities as a digital citizen, including awareness of dangers and managing their online identities (digital footprint).
- To reinforce within the school community what bullying is (including cyberbullying), and the fact that it is unacceptable.
- Everyone within the school community to be alert to signs and evidence of cyberbullying and to have a responsibility to report it to staff, whether as observer or victim.
- To ensure that all reported incidents of cyberbullying are investigated appropriately and that support is given to both victims and perpetrators.
- To seek parental and peer-group support and co-operation at all times.

Implementation:

- Students and teachers will be made aware of our school's eSmart guidelines.
- Students and teachers will work through/discuss these issues using our school's ICT Scope and Sequence.
- Parents, teachers, students and the community will be aware of the school's position on cyber-bullying. Teachers will be regularly reminded of their duty of care regarding protection of students from all forms of bullying.
- The school will adopt a four-phase approach to bullying;

A. Primary Prevention:

- Professional development for staff relating to all forms of bullying including cyberbullying, harassment and proven counter measures.
- Educate the school community about the seriousness of cyberbullying, its impact on those being bullied and how this behaviour is unacceptable
- Community awareness and input relating to bullying (including cyberbullying), its characteristics and the school's programs and response.
- Provide programs that promote resilience, life and social skills, assertiveness, conflict resolution and problem solving.
- Provide eSmart curriculum to all students, as outlined on the ICT Scope and Sequence plan.
- Each classroom teacher to clarify with students at the start of each year the school policies in relation to bullying, cybersafety and eSmart guidelines.

References: Safe Schools are Effective Schools booklet

www.curriculum.edu.au/mindmatters

S428-2007 Cyber Bullying – Updating the Student Code of Conduct

www.bullyingnoway.com.au

<http://www.education.vic.gov.au/management/elearningsupportservices/www/classroom/cyberbullying.htm>

- All students to be provided with individual and confidential computer and network log ins and passwords. Processes to be put in place to ensure tracking of student activity on the school's computer equipment and network. Firewalls to be installed to eliminate outside traffic into the school's network and intranet.
- Students to be aware of Quarry Hill User Agreement Policy.

B. Early Intervention:

- Encourage children and staff to report cyberbullying incidents involving themselves or others.
- Classroom teachers and principal on a regular basis remind students and staff to report incidents of cyberbullying.
- Regular monitoring of traffic on school's computer networks to identify potential problems.
- Parents encouraged to contact school if they become aware of a problem.
- Recognition and reward for positive behaviour and resolution of problems.

C. Intervention:

- Once identified each bully, victim and witnesses will be spoken with, and all incidents or allegations of bullying will be fully investigated and documented.
- Parents to be contacted.
- Students and staff identified by others as bullies will be informed of allegations.
- Both bullies and victims will be offered counselling and support.
- Removal of cyberbullies from access to the school's network and computers for a period of time.
- If student bullying persists parents will be contacted and consequences implemented consistent with the school's Student Code of Conduct.

D. Post Violation:

- Consequences for students will be individually based and may involve:-
 - exclusion from class.
 - exclusion from yard.
 - school suspension.
 - withdrawal of privileges.
 - ongoing counselling from appropriate agency for both victim and bully.
- Criminal charges being laid by police.
- Support Structures.
- Ongoing monitoring of identified bullies.
- Rewards for positive behaviour.

Date Implemented	June 2016
Author	ICT Committee
Approved By	School Council
Date Reviewed	June 2016
Responsible for Review	ICT Committee
Review Date	June 2018

References: Safe Schools are Effective Schools booklet
www.curriculum.edu.au/mindmatters

S428-2007 Cyber Bullying – Updating the Student Code of Conduct
www.bullyingnoway.com.au

<http://www.education.vic.gov.au/management/elearningsupportservices/www/classroom/cyberbullying.htm>