

## California Gully Primary School 123

# CYBERSAFETY

### Rationale:

Internet and digital technologies are now very much a part of life and learning. As an increasingly interactive medium, digital technologies bring with them exciting new opportunities to engage children and young people in their learning. At the same time these technologies also bring some risks. Increasingly schools are dealing with incidents of cyberbullying or unacceptable behaviour that have occurred in the online world or using technology such as mobile phones.

The school will promote a positive culture where bullying is not accepted, and in so doing, all will have the right of respect from others, the right to learn, teach or work, and a right to feel safe and secure in their school environment.

### Definition

*Cybersafety* is the *safe and responsible* operation/use, at any time, on or off the school premises by any person, of the school's Internet facilities, network and associated ICT equipment/devices, such as computers and laptops, digital cameras, mobile phones and other devices.

*Bullying* is when someone repeatedly and deliberately hurts or upsets someone else. This may involve verbal, physical, relational and psychological forms of bullying.

*Cyber bullying* involves the use of information and communication technologies such as e-mail, SMS messages, digital images, instant messages and websites to engage in the bullying of other individuals or groups. This technology provides an alternate means of verbal, physical, relational and psychological forms of bullying. (Refer Appendix C)

### Purpose

California Gully Primary School will develop and maintain rigorous and effective cybersafety practices which aim to maximise the benefits of the Internet and ICT devices/equipment to student learning and to the effective operation of the school, while minimising and managing any risks.

- 1.1 To provide a positive culture at our school where bullying is not accepted, and in doing so, all will have the right of respect from others, the right to learn or teach, and a right to feel safe and secure. (see Appendix B)
- 1.2 To ensure that the members of the school community are aware of these rights and responsibilities.
- 1.3 To assist students to take full responsibility and be aware of the consequences of their actions.
- 1.4 To make the school community aware that cyber bullying is a criminal offence, which is covered by various State and Commonwealth laws. (Refer to Appendix A)

### Guidelines

- 2.1 To ensure that all students, parents/guardians, staff and the wider community work cooperatively to eliminate cyberbullying.
- 2.2 All school and other community members have the responsibility to prevent and report observations of cyber bullying in order to ensure that their right to a safe and supportive learning environment occurs.
- 2.3 The use of the internet and ICT devices /equipment by staff, student and other approved users is to be limited to educational, professional development and personal usage appropriate in the school environment.
- 2.4 The school has **the right to monitor, access and review all use of ICT equipment at all times**. This would include personal e-mails and messages sent and received on the school computers, on social media, in chat rooms and on network facilities.
- 2.5 The school has **the right to audit any material at any time**, on school owned equipment or privately owned ICT devices brought to school.
- 2.6 The safety of the students is paramount and **any apparent breach of cybersafety will be taken seriously**.
- 2.7 To continually educate the school community to ensure a cybersafe school environment is maintained.

## **Implementation**

- 3.1 The encouragement of cybersafe behaviour across the school including 'Acceptable Use Agreements'
- 3.2 The school cybersafety practices and procedures will be followed in response to any incidents. Advice will be sought from appropriate sources including the police and DEECD in relation to serious incidents. If illegal material or activities are suspected, the matter will be reported to the relevant law enforcement agency
- 3.3 The community will be made aware of the school's cybersafety procedures in a variety of ways eg school web site , the newsletter.
- 3.4 The school will have processes in place to monitor access through filtering and tracking tools, but cannot guarantee isolation from potentially undesirable material or communication.
- 3.5 The school will provide relevant education in cybersafety for students, staff and parents on a regular basis.
- 3.6 Parents have the responsibility and the right to supervise their child's access to online use and establish safety procedures that prohibit bullying.
- 3.7 Staff and parents need to set a positive example when dealing with bullying.
- 3.8 The school community will provide access to a safe environment, culture and information that supports the building of resilience and the support to identify and stop bullying.

## **Evaluation**

- 4.1 A short review will take place one year after the policy has been approved by School Council.
- 4.2 An extensive review to take place in 3 years.

## **Appendix**

### **(A) The numerous State and Commonwealth laws which cover cyber crime include:**

The Commonwealth's Criminal Code Act 1995, section 4.7.4.17 notes that it is an offence for a person "to use a carriage service to menace, harass or cause offence."

The Commonwealth's Criminal Code Act 1995, 4.7.4.15 notes that it is an offence for a person "to use a carriage service to make a threat"

The Commonwealth's Criminal Code Act 1914, part VIIB, section 85ZE , 17 notes that it is an offence for a person knowingly or recklessly use a telecommunications service supplied by a carrier in such a way as would be regarded by reasonable persons, being in all circumstances, offensive."

The Victorian Crimes Act 1958 was amended in 1995 to include an offense of "stalking". This includes telephoning and sending electronic messages with the intention of causing physical and mental harm.

The sending of images is also covered by various State and Commonwealth laws that prevent the publication of material that is objectionable, unclassified or unsuitable for minors.

### **(B) The California Gully Bullying Policy**

### **(C) Examples of Cyber bullying and harassment using websites, mobile phones, chat rooms and SMS and other devices may include:**

- \*posting of humiliating messages or pictures or spreading rumours
- \*excluding of people, encouraging others to delete a person from friendship lists setting up closed groups and ignoring messages.
- \*forwarding on of students private communication.
- \*manipulating someone to reveal personal information.
- \*sending threatening messages.
- \*communicating under false pretences.

### **Evaluation:**

This policy will be reviewed as part of the school's three-year review cycle.

This policy was last ratified by School Council in 2013