

Resurrection School: Cyber-Safety Policy

The overall goal of Resurrection School is to create and maintain a cybersafety culture that is in keeping with our values and with legislative and professional obligations. This policy is in alignment with other wellbeing and school policies. The Acceptable Use Agreement (AUA) for staff and students outlines the obligations, responsibilities, and the nature of possible consequences associated with cybersafety breaches that undermine the safety of members of the school community and beyond.

E-learning and Information Communication and Technology (ICT) equipment / devices bring great benefits to the teaching and learning programs at Resurrection School, and to the effective operation of the school. The ICT equipment is for educational purposes appropriate to this environment, whether it is owned or leased either partially or wholly by the school, and used on or off the site.

The measures to ensure the cyber-safety of students & staff are based on our school values: to be FAIR: friendly, assertive, inclusive, respectful and responsible. All students will be issued with an annual AUA and once signed consent has been returned to school, students will be able to use the school ICT equipment.

Rigorous cyber-safety practices are in place, which include the annual cyber-safety AUA for staff and students, who have been involved in the development of the agreement. Child protection education, eSmart protection curriculum, includes information about remaining safe when using technologies and is provided to staff, students and parents.

Material sent and received using the network **and blogging** may be monitored and filtered. Monitoring software may be used to restrict access to certain sites and data, including e-mail. Where a student is suspected of a cyber safety incident the Resurrection School Cyber Safety Action Flow Chart is to be used.

Important terms:

'**Cyber-safety**' refers to the safe use of the Internet and ICT equipment / devices, including mobile phones.

'**Cyber bullying**' is bullying which uses echnology as a means of victimising others. It is the use of an Internet service or mobile technologies, including social networking services (eg Facebook, MySpace, Twitter) with the intention of harming another person.

'**School ICT**' refers to the schools computer network, Internet access facilities, computers, and other ICT equipment / devices as outlined below.

'**ICT equipment / devices**' includes computers (such as desktops, laptops, PDAs), storage devices (such as USB and flash memory devices, CDs, DVDs, floppy disks, audio players), cameras, mobile phones, gaming consoles, video and audio players / receivers, and any other similar technologies.

'**Inappropriate material**' means material that deals with matters such as inappropriate language, images or information.

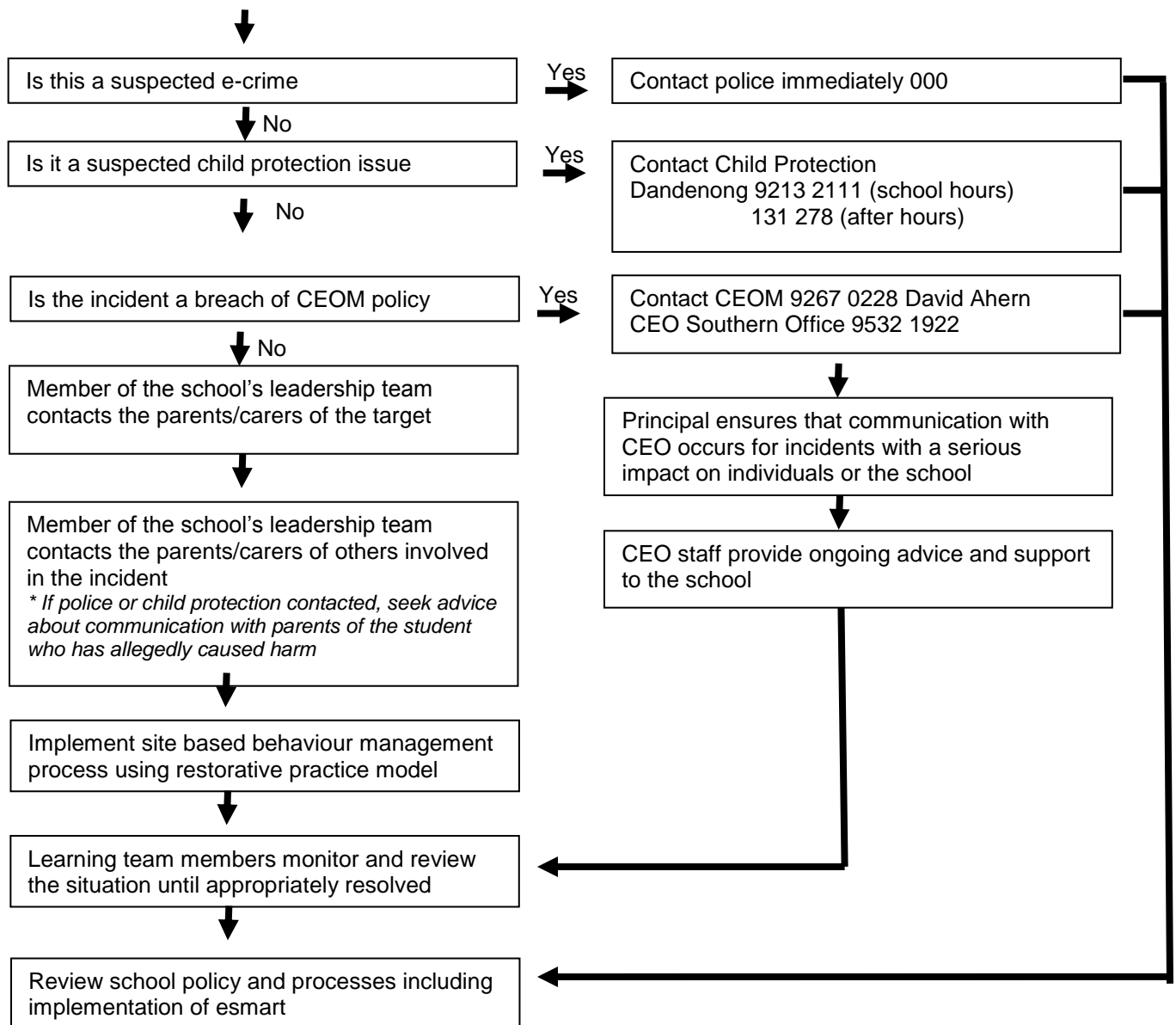
'**E-crime**' occurs when computers or other electronic communication equipment / devices (eg Internet, mobile phones) are used to commit an offence, (are targeted in an offence, or act as storage devices in an offence.) such as bullying, photos or words

Resurrection School Cyber Safety Action Flow Chart

There is a cyber safety incident. This could occur on or offsite and / or out of school hours. Incident reported to a staff member. Incident referred to leadership team member.

Information gathered by leadership team member in initial interview to include:

- The nature of incident
- Person/s involved
- **Hardcopy of evidence to be taken**
- All involved staff document the report of the incident, the response and their actions



If more information becomes available at any stage, return to previous steps if appropriate.

Useful websites

Cybersmart: www.cybersmart.gov.au

Cybersmart provides activities, resources and practical advice to help young kids, kids, teens and parents safely enjoy the online world. Developed by the Australian Communications and Media Authority, Cybersmart is part of the Australian Government's cybersafety program.

ThinkUKnow: www.thinkuknow.org.au

ThinkUKnow is an Internet safety program delivering interactive training to parents, carers and teachers through primary and secondary schools across Australia using a network of accredited trainers.

eSmart www.esmartschools.org.au/Pages/eSmartPortal.aspx

eSmart aims to make cybersafety a normal part of everybody's life by equipping them to use technologies in ways that are positive and that protect them from the potential risks.

Cyber Safety Solutions www.cybersafetysolutions.com.au

Susan McLean, Australian cyber safety expert. Offers a level of cyber assistance to parents kids and schools

NetSmartz www.NetSmartz.org

Recommended by Susan McLean as excellent content. Internet safety program in USA

Bullying.org www.bullying.org

Bullying.org's purpose is to prevent bullying in our society through education and awareness.

Learning On Line www.education.vic.gov.au/learningonline

The Learning On Line website presents the Department of Education and Early Childhood Development's advice for schools on cybersafety and educating young people to be responsible users of mobile and digital technologies.

i-SAFE www.iSafe.org

i-SAFE Inc. is a leading publisher of media literacy and digital citizenship education materials and programming with worldwide distribution channels.

Netlingo <http://www.netlingo.com/acronyms.php>

A comprehensive list of Chat Acronyms & Text Message Shorthand