Government of South Australia

Making our sites SAFER

GUIDELINES FOR SITE LEADERS

No 7, Published August 2010, Updated 11/11

E-CRIME

This document provides a summary of actions that schools should follow in the case of an e-crime. It is not intended to replace the DECD policy document Cyber-safety – Keeping Children Safe in a Connected World that details legislation, policy and practice, but to provide a step by step guide for action.

WHAT IS AN E-CRIME?

E-crime occurs when computers, mobile phones or other electronic communication devices are used to commit an offence, are targeted in an offence, or act as a storage device in an offence. An e-crime can include sexting (see below), impersonation, intimidation, harassment and using the internet or mobile phones to transmit suicide-related material, to make a threat or to menace, harass or cause offence.

Sexting occurs when a person takes a sexually-explicit digital photograph and/or transmits this image. If the image is of a minor, it may represent child pornography, that can result in imprisonment.

Cyber bullying, e-crime and the protection of children and young people: Advice for families provides further details related to e-crime.

RESPONSIBILITIES OF LEADERS WHEN THERE IS A SUSPECTED E-CRIME:

- Report incident to SAPOL 131 444 and follow their advice. Document actions.
- Confiscate the equipment (eg mobile phone) and hand over to the SAPOL investigating officer.
- Do **not** open or view any evidence as this may compromise the investigation.
- Cease any further investigation of the e-crime.
- Contact Regional Office and School Care 8463 6568. Submit a Critical Incident Report (IRMS).
- If SAPOL do not proceed with the investigation treat the incident as a student behaviour management issue.
- Where the incident is perpetrated by a student and affects the wellbeing of other students or staff members, leaders should follow the school discipline procedures. (See CE Circular DECS 09/3677)

RESPONSIBILITIES OF LEADERS WHEN THERE IS A SUSPECTED CHILD PROTECTION ISSUE

Where a cyber incident occurs from an adult to a child it is a child protection issue and it must be reported to the Child Abuse Report Line on 13 14 78 and, if appropriate, SAPOL on 131 444. Your Regional Office should also be advised and a Critical Incident Report submitted through IRMS..

RESPONSIBILITIES OF LEADERS WHEN ONLINE STUDENT BEHAVIOUR THREATENS THE WELLBEING OF A STUDENT OR STAFF MEMBER

If a child or student behaves online in a manner that threatens the wellbeing of another student, even if this occurs off-site and/or out of school hours, the principal has the authority under Regulations 41.1.b to suspend or exclude a student from attendance at school.

As part of the suspension or exclusion conference, negotiation should include the permanent removal of offensive or abusive material. Where possible a copy of the content should be maintained.

If the child attends a preschool, then the preschool director is guided by Supporting and managing children's behaviour: An early childhood resource. If required, contact School Care on 8463 6568, for advice on the most appropriate action.

Where offensive and untrue material about a teacher is placed on the internet, as a result of their role as a teacher, the school should do all it can to support the teacher, including having the material removed. Where possible a copy of the content should be maintained. Sites requiring support to copy content should contact School Care on 8463 6568 for assistance.

When approached most members of the community will remove offensive material, as they are unaware that those in authority can retrieve all postings. Legal advice from DECD Legislative and Legal Services 8226 1555 is available if required.

SOCIAL NETWORKING SITES COMPLAINT PROCESSES

Services such as *Facebook*, *YouTube* and *Rate My Teacher* have complaints processes. To access these processes and to report a complaint you need to be a member of the service. Sites could consider nominating members of the leadership team to join various social networking services to enable sites prompt and easy access to complaint processes. When complaining provide the URL, the name of the perpetrator, their age (if a student) and the request. Monitor the site to see when the content is removed and inform those involved.

These services have conditions of membership. For example Facebook members are required to be no younger than 13 years old to have an account. If a student has falsified their age they have violated a condition of use and can have their site removed by the service administrator.

The Australian Communication and Media Authority (ACMA) administers a national regulatory scheme and responds to community concerns about offensive and illegal material online.

If a community member finds offensive material on the internet or on an electronic device, they can make a report to the ACMA. Go to www.cybersmart.gov.au click on the *Cybersafety Help* button and they will be guided by prompts to make a complaint.

OTHER USEFUL WEBSITES

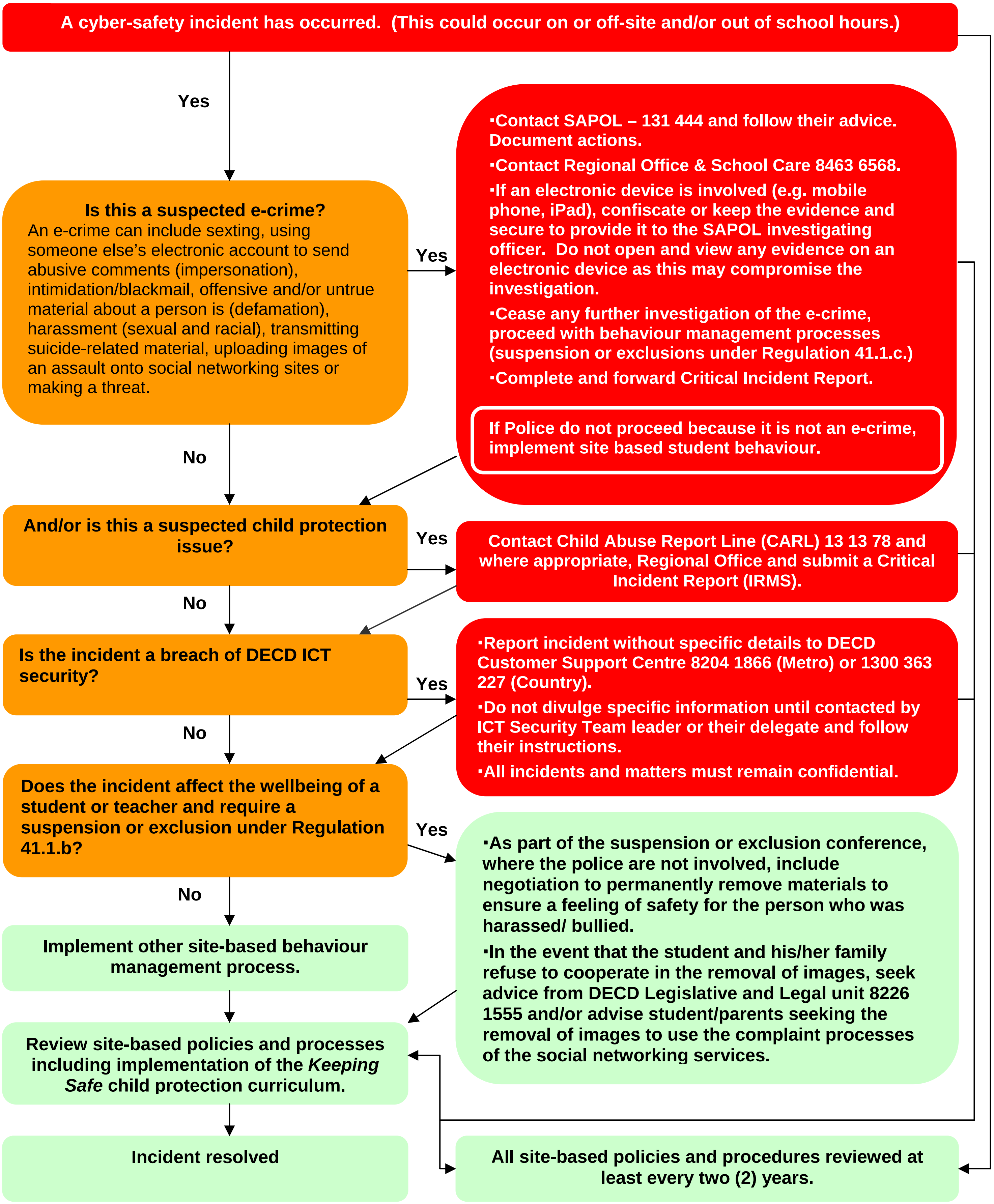
- Bullying No Way! www.bullyingnoway.com.au
- Child and Youth Health www.cyh.com
- DECD cyber safety web page http://www.decd.sa.gov.au/speced2/pages/cybersafety/36219/
- Kids Helpline www.kidshelp.com.au
- ThinkUKnow the Australian Federal Police internet safety program www.thinkuknow.org.au
- The Australian Government's *Cyber safety help button* http://www.dbcde.gov.au/online_safety_and_security/cybersafetyhelpbutton_download

FURTHER INFORMATION AND SUPPORT

Further information and support can be provided from the DECD Child and Student Wellbeing unit on 8226 1323.

Making our sites SAFER

Cyber – Safety Guidelines to assist in decision making



A cyber-safety incident has occurred. (This could occur on or off-site and/or out of school hours.)

Yes

Is this a suspected e-crime?
An e-crime can include sexting, using someone else's electronic account to send abusive comments (impersonation), intimidation/blackmail, offensive and/or untrue material about a person is (defamation), harassment (sexual and racial), transmitting suicide-related material, uploading images of an assault onto social networking sites or making a threat.

Yes

- Contact SAPOL – 131 444 and follow their advice. Document actions.
- Contact Regional Office & School Care 8463 6568.
- If an electronic device is involved (e.g. mobile phone, iPad), confiscate or keep the evidence and secure to provide it to the SAPOL investigating officer. Do not open and view any evidence on an electronic device as this may compromise the investigation.
- Cease any further investigation of the e-crime, proceed with behaviour management processes (suspension or exclusions under Regulation 41.1.c.)
- Complete and forward Critical Incident Report.

If Police do not proceed because it is not an e-crime, implement site based student behaviour.

No

And/or is this a suspected child protection issue?

Yes

Contact Child Abuse Report Line (CARL) 13 13 78 and where appropriate, Regional Office and submit a Critical Incident Report (IRMS).

No

Is the incident a breach of DECD ICT security?

Yes

- Report incident without specific details to DECD Customer Support Centre 8204 1866 (Metro) or 1300 363 227 (Country).
- Do not divulge specific information until contacted by ICT Security Team leader or their delegate and follow their instructions.
- All incidents and matters must remain confidential.

No

Does the incident affect the wellbeing of a student or teacher and require a suspension or exclusion under Regulation 41.1.b?

Yes

- As part of the suspension or exclusion conference, where the police are not involved, include negotiation to permanently remove materials to ensure a feeling of safety for the person who was harassed/ bullied.
- In the event that the student and his/her family refuse to cooperate in the removal of images, seek advice from DECD Legislative and Legal unit 8226 1555 and/or advise student/parents seeking the removal of images to use the complaint processes of the social networking services.

No

Implement other site-based behaviour management process.

Review site-based policies and processes including implementation of the *Keeping Safe* child protection curriculum.

Incident resolved

All site-based policies and procedures reviewed at least every two (2) years.

Regional Offices together with School Care can provide additional support if required.