Further information

For further information on cyberbullying and positive online behaviour in a school context, contact The Department of Education, Training and Employment:

Incident management:
CyberSafety.ReputationManagement@dete.qld.gov.au

Cybersafety website:
www.education.qld.gov.au/studentservices/behaviour/qsaav/cybersafety.html

Support and advice can also be found from the following organisations and initiatives:

Cybersmart: Advice for parents
www.cybersmart.gov.au/Parents.aspx

Facebook: Be Bold. Stop Bullying.
www.facebook.com/beboldstopbullyingau

Kids Helpline
www.kidshelp.com.au/grownups

Parentline
www.parentline.com.au

Bullying. No way!
www.bullyingnoway.gov.au

Queensland Police Service:
Who's chatting with your kids? / Surf Safely
www.police.qld.gov.au/programs/cscp/personalSafety/children

Australian Federal Police:
ThinkUknow
www.thinkuknow.org.au

Stay Smart Online
www.staysmartonline.gov.au

Department of Broadband, Communications and Digital Economy — Easy Guide to Socialising Online
www.dbcde.gov.au/easyguide

Digital Parenting — Vodafone
www.vodafone.com/content/index/parents

Licence

This cybersafety and cyberbullying guide is licensed by the State of Queensland (Department of Education, Training and Employment) under a Creative Commons Attribution (CC BY) 3.0 Australia licence.

CC BY Licence Summary Statement

In essence, you are free to copy, communicate and adapt this guide, as long as you attribute the work to the State of Queensland (Department of Education, Training and Employment).

To view a copy of this licence, visit: www.creativecommons.org/licenses/

Attribution

Content from this guide should be attributed as:

The State of Queensland (Department of Education, Training and Employment) Cybersafety and cyberbullying a guide for parents and caregivers 2013.

Images

All images included in this manual are identified as 'restricted' and the following terms apply:

You may only use this image (in its entirety and unaltered) as an integrated part of this entire guide or as an unaltered integrated part of an extract taken from this guide.

For updated copies of this document, and other cybersafety resources, please visit
www.education.qld.gov.au/studentservices/behaviour/qsaav/info-parents.html

Social media

and the school community

This guide offers some information to parents and caregivers about how to use social media in relation to comments or posts about their school community.

The internet, mobile phones and social media provide wonderful opportunities for you to network and socialise online. While these technologies provide positive platforms for sharing ideas, they also have the potential to cause pain and suffering to individuals, groups or even whole communities.

Just as you would discourage your child from behaving inappropriately online, it's important to remember that sometimes negative comments that parents and caregivers post about their school community have a greater impact than expected.

Reputations of teachers, schools, principals and even parents can be permanently damaged — and in some cases, serious instances of inappropriate online behaviour are dealt with by police and the court system.

Queensland Government

General tips

Being aware of a few simple strategies can help keep the use of social media positive and constructive:

- Before you post something online, ask yourself if the community or individual really need to know. Is it relevant, positive and helpful?
- Remember that what you post online is a direct reflection of who you are. People will potentially form lasting opinions of you based on what you post online.
- Be a good role model. If things get heated online consider logging out and taking a few moments to relax and think. Hasty, emotive responses could inflame situations unnecessarily.
- Be mindful when commenting, try to keep general and avoid posting anything that could identify individuals.
- A few years ago parents may have discussed concerns or issues with their friends at the school gate. Today with the use of social media, online discussions between you and your close friends can very quickly be shared with a much wider audience, potentially far larger than intended.
- Taking a few moments to think about the content you are about to post could save upset, embarrassment, and possible legal action.
- As a parent you have a role in supervising and regulating your child's online activities at home and its impact on the reputation and privacy of others. Parents are their child's first teachers — so they will learn online behaviours from you.

Is it appropriate to comment or post about schools, staff or students?

- Parental and community feedback is important for schools and the department. If you have a compliment, complaint or enquiry about an issue at school, the best approach is to speak directly to the school about the matter, rather than discussing it in a public forum.
- While many schools use social media to update parents of school notices, the department prefers that parents contact schools directly with a compliment, complaint or enquiry due to privacy considerations. Imagine if your doctor, accountant or banking institution tried to contact you to discuss important matters via Facebook.
- If you have raised an issue with a school or know that another person has, consider refraining from discussing those details on social media, particularly the names of anyone involved.
- Keep comments calm and polite, just as you would over the telephone or by email.
- If you encounter negative or derogatory content online which involves the school, hinders a child's learning and/or affects the school community at large, contact the school principal.

Possible civil or criminal ramifications of online commentary

A serious instance of inappropriate online behaviour may constitute a criminal offence and become a police matter. For example, online content may substantiate the offence of 'using a carriage service to menace, harass or cause offence' ***(Criminal Code Act 1995 (Cth) s. 474.17)***.

School staff may contact their union or obtain personal legal advice if they feel that online content seriously impacts their reputation. Defamatory online content may give rise to litigation under the ***Defamation Act 2005 (Qld)***.

What about other people's privacy?

If you upload photos of your children, be mindful of who might be in the background. You might be happy to share your child's successes with your friends and family via social media, but some parents are not.

If you are tagging or naming students, consider that other parents may not want their child's name attached to images online.

Get to know
social media

Take some time to research online networks and mobile apps, in particular the:

- terms of use
- common features and terminology
- policies for the removal of content
- privacy settings.

Search online networks for useful links such as safety centres, forms for reporting inappropriate content and terms and conditions. It may be helpful to bookmark these pages.

What if
I encounter problem content?

Taking the following steps may help resolve the issue in a constructive way:

- refrain from responding
- take a screen capture or print a copy of the concerning online content
- if you consider problem content to be explicit, pornographic or exploitative of minors, you should keep a record of the URL of the page containing that content but NOT print or share it. The URL can be provided to the school principal, or police, as needed for escalation of serious concerns
- block the offending user
- report the content to the social media provider.

How do I report
inappropriate content?

Social media providers may remove content that contravenes their terms of service and/or acceptable use policies. Most websites and apps have a 'report/block this person' or 'report/flag content' function.

Common links
for reporting social media content

Facebook
www.facebook.com/safety

Instagram
http://help.instagram.com

Google including YouTube
www.google.com/support/go/legal

Snapchat
http://support.snapchat.com

Twitter
https://support.twitter.com

Further information

Australian Communications Media Authority (ACMA) Cybersmart program
www.cybersmart.gov.au/Parents.aspx

Bullying No Way!
www.bullyingnoway.com.au/parents

Creep Quiz – Are you safe online?
http://creepquiz.eq.edu.au/

Google Safety Center
www.google.com/safetycenter

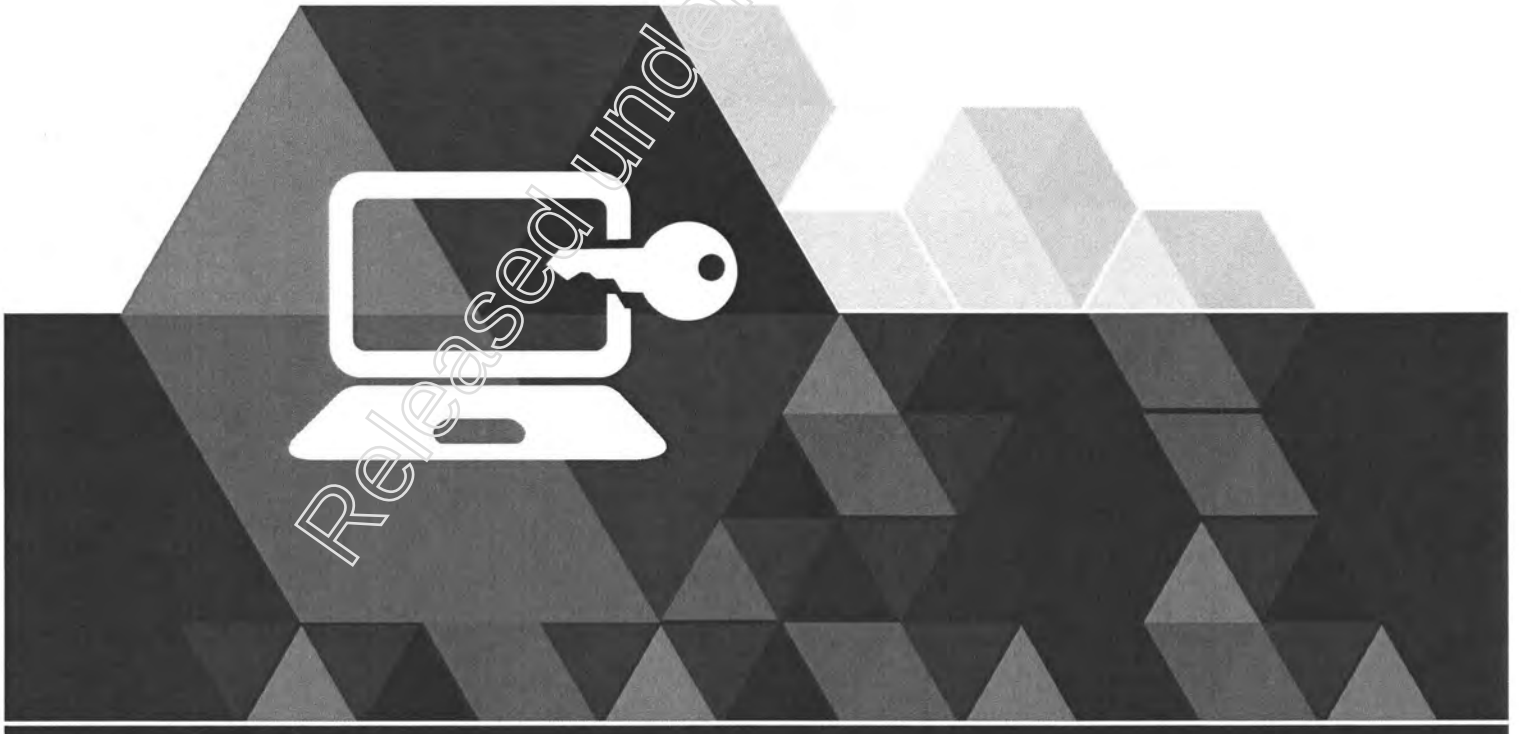
Young and Well Cooperative Research Centre
www.youngandwellcrc.org.au

For further information and cybersafety resources, please visit
www.deta.qld.gov.au/cybersafety

This document was commissioned by
Learning Technologies, Web and Digital Delivery

Cyberbullying
and reputation management

Incident management guidelines for principals



February 2013

Queensland Government

Contents

Overview

This document provides information for Queensland State School principals and other school staff on initial responses to incidents related to cyberbullying and other forms of inappropriate online activity used against students and staff members.

It also provides advice for school administration staff on how to deal appropriately with the technical aspects of incidents involving mobile phones, portable devices, laptop computers and other electronic devices.

A school's approach to cyberbullying and reputation management

Cyberbullying is when technology, such as email, mobile phones, chat rooms and social networking sites, are used to verbally or socially bully another person. Bullying is an ongoing abuse of power to threaten or harm another person.

Reputation Management is the process of monitoring, addressing or mitigating online content about an individual staff member or school. Anything that is posted about an individual or organisation online forms part of their 'digital reputation'. This digital reputation can then have an effect on the individuals/organisations offline reputation.

In managing a cyberbullying or reputation management incident, the primary concern must be the welfare of the student and staff members affected.

All incidents that directly impact on the good order and management of the school should be managed in accordance with Department of Education, Training and Employment (the Department) policies and procedures. A complete, objective and efficient investigation of the incident is critical in achieving outcomes that are ethical, follow departmental policy and afford natural justice to all parties involved.

As well as implementing effective incident responses, schools should adopt a proactive approach that includes:

- a whole school cybersafety framework
- up-to-date behaviour management documents such as the **Responsible Behaviour Plan for Students (RBPS)** and ICT Acceptable Use Agreements
- clear directions about the permissible use of mobile phones and other electronic equipment by students during school hours ***(see* Appropriate use of mobile telephones and other electronic equipment by students)**
- clear descriptions of the types of behaviours that occur outside of school hours and off premises that affect the good order and management of the school. These should be included in the RBPS and frequently communicated to students.

Incident management response

The types of incidents covered by this document are described in Appendix 1.

1. The principal should firstly determine **whether the incident impacts on the good order and management of the school**. This impact will need to be assessed at an individual school level.

Note: You are welcome to acquire further advice and assistance by contacting the Principal Advisor, Cybersafety and Reputation Management, Learning Technologies Unit by phoning (07) 3421 6335 or emailing CyberSafety.ReputationManagement@deta.qld.gov.au

If it is determined the incident will be investigated and managed by the school then the following steps are recommended

2. Assess the incident to **determine the level of threat** to the student or staff member. The physical safety and emotional well-being of the people involved is the primary concern throughout the incident management process.

Note: You may refer any staff member to the Employee Assistance Service (EAS) which provides a range of supportive psychological health services to employees including confidential counselling *(See Queensland Government contacts on page 13).*

3. **Initiate an incident response** immediately. Start an incident management log (running sheet) which records times and dates of events, observations, tasks completed, persons involved and written conversational notes. This information will need to be retained if the school is seeking to take disciplinary action against a student or a referral to police is made.

Note: A Principal should be mindful throughout the incident response of the reporting of harm obligations under the Department's Student Protection and Allegations against employees in the area of student protection policies.

4. **Gather and preserve any evidence** of inappropriate behaviour or a potential crime, where legally permissible. This includes confiscating electronic devices such as mobile phones, portable devices or laptop computers if permissible under DETE policies *(see How to preserve evidence on page 8).*

   If the material in question is child exploitation material the police should be notified and staff should make no attempt to save, copy or otherwise deal with the material (*see Appendix 2 - Offences involving child exploitation material).*

Note: A principal or staff member does not have the authority to open, search or otherwise deal with the property of a student without the consent of the student or a parent of the student. For example, a principal or staff member who removes a mobile phone from a student is not authorised to unlock the phone or to read, copy or delete messages stored on the phone – refer to policy Temporary removal of student property by school staff.

5. If evidence of inappropriate behaviour or online activities that maybe a potential crime ***(see Appendix 2 - Offences involving child exploitation material)*** is found, **report the incident to police** and provide them with any evidence you have gathered. Any further evidence gathering by departmental staff should cease unless police advise otherwise, however, principals may continue to investigate the matter for disciplinary purposes, subject to all laws and department policies.

Notes:

a. Local police handling this incident may need to be alerted to the fact that support and specialist advice can be obtained from their Child Protection Investigation Unit or the Hi-Tech Crime Investigation Unit which is attached to the Fraud and Corporate Crime Group of State Crime Operations Command.

b. While some content may be upsetting for a student or parent, it may not constitute a criminal offence or grounds for taking disciplinary action, and a student's or parent's expectations of swift action by police or the Department may be unrealistic. Schools should therefore advise parents of ways to remove upsetting or inappropriate content from a variety of online environments and how to safeguard their child from cyber-attacks.

c. Police require the child/staff member to make a complaint, a school cannot make a complaint on behalf of the child/staff member.

6. If the principal determines the online activity **is not of a criminal nature**, steps should be taken to have upsetting or inappropriate **content removed as soon as possible**. *Please refer to the 'Removal of content' section of this document on page 10.*

Notes:

a. If the student(s) responsible refuses to remove the content or the content is still showing in search engines after removal, contact the service provider or site administrator and ask them to remove the content and all references to it. A link to the site administrator can usually be found on the bottom of a website page or under a 'contacts' tab.

b. If the identity of the student(s) responsible is unknown, school staff should read postings and comments in an attempt to identify individuals from nicknames, initials, date of birth or other possible identifying features used in profiles and discussions. Ask the service provider or site administrator to remove the content and all references to it. If the host/site administrator contact details can't be located on the web site, contact the DETE Service Centre on 1800 680 445 for assistance.

c. If the website site administrator/owner refuses to remove the content, the domain host (owner of the host server) can be asked to remove the content or close the website.

continued on next page

7. **Report it to the Department** *(see Reporting on page 11).*

8. If it is determined that the behaviour of one or more students constitutes cyberbullying or other unacceptable behaviour, then **appropriate follow up action should be taken** in accordance with the school's Responsible Behaviour Plan for Students (RBPS) and Behaviour Management Program.

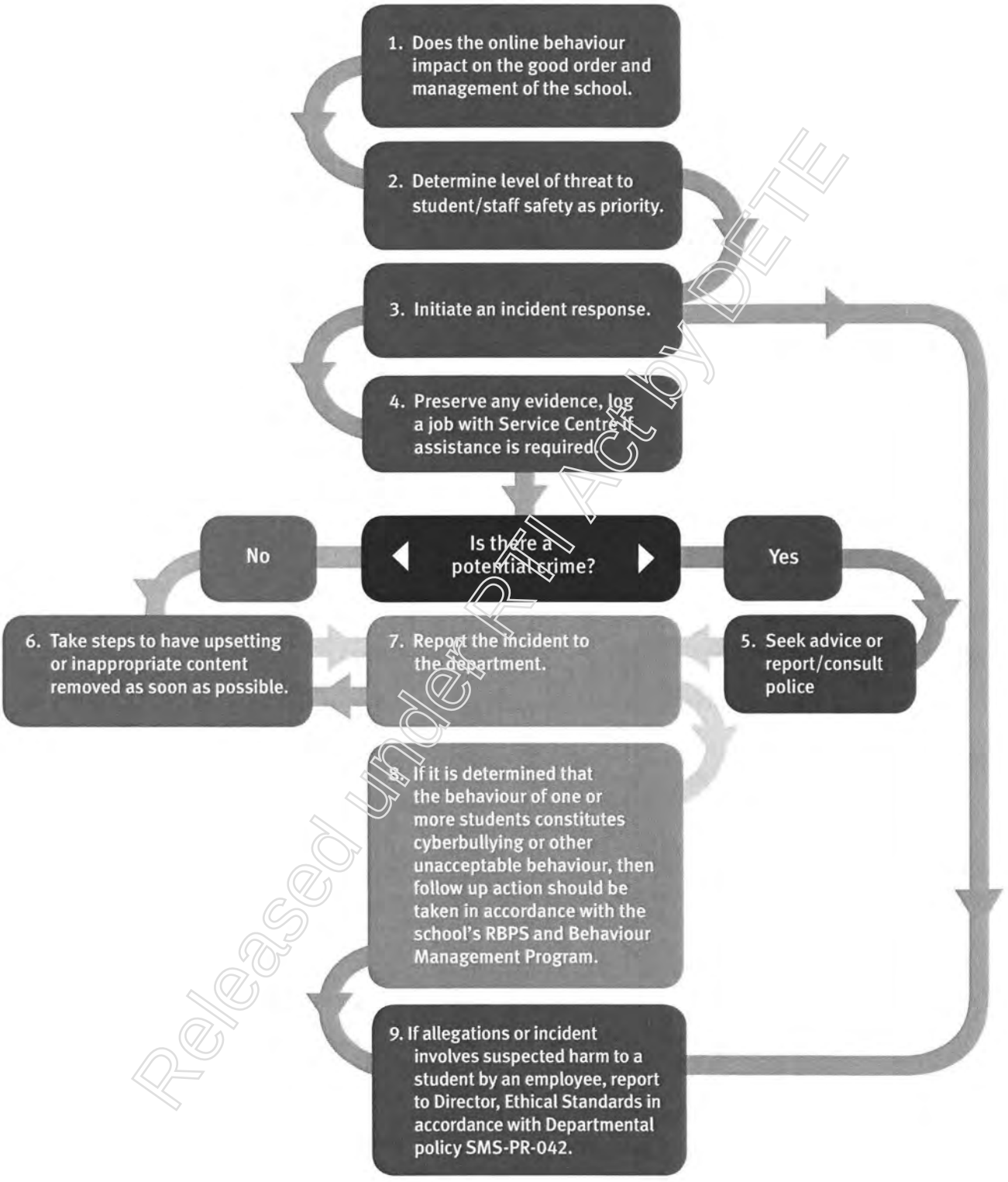
9. A Principal should be mindful if the allegations or the incident involves suspected harm to a child/student by an employee, policy requires the principal to report the incident to the Director, Ethical Standards. For further information refer to policies **Student Protection** and **Allegations against employees in the area of student protection.**

For assistance with any stage of this process contact the Service Centre either by

Telephone: 1800 680 445
Email: **servicecentre@deta.qld.gov.au**
Web: **https://qlddet.service-now.com/**

To escalate the job to the Cybersafety and Reputation Management Team, Learning Technologies unit *(See Queensland Government contacts on page 13)*

Incident management response flowchart



How to preserve evidence

The school should preserve any evidence of the incident, where legally permissible. As noted above, staff should make no attempt save, copy or otherwise deal with any child exploitation material. ***See Appendix 2 - Offences involving child exploitation material.***

Depending on the nature and seriousness of the incident, evidence may also be required by parents or other officers in the Department.

When gathering evidence:

- do not delete text messages, emails, instant messages, voicemail, web pages, social media profiles or other digital content that is causing concern
- save emails and/or take screen shots of inappropriate internet content and save in a secure location. This should be done as soon as possible
- where possible, record any sender identification, such as username, social media account, email, or mobile phone number
- record the time, date and URL of the web site (in the screen shot if possible), consider whether to confiscate mobile phones and other electronic equipment that may have been used in an incident.

  Note: confiscation can only be undertaken if in accordance with Appropriate Use of Mobile Telephones and other Electronic Equipment by Students and Temporary removal of student property by school staff.

Police involvement

If the incident has been reported to the police as a potential crime, then the police have powers to obtain the alleged offender's identifying information from various sources including internet service providers, mobile phone companies, social networking or webmail providers.

When the police are involved, school staff should retain evidence as suggested in the section above. They should not however, attempt to examine, touch or tamper with the evidence. Doing so, could make it unacceptable for investigations, where someone else, and not the offender, is the last person to handle the device or item.

Police follow examination procedures which do not alter the original evidence. If the material, text message or image has been deleted from the electronic device, police may engage specialist units to attempt to recover this evidence through forensic examinations.

Suggested methodology for preserving evidence

The following are some recommendations for keeping the various types of evidence safe following its implication in a crime.

 Social networking sites such as Facebook	Take **screen shots** of content, ensuring the time, date and website URL are recorded and saved to a secure location.
 Video hosting sites such as YouTube	**Windows users:** hold down the 'Ctrl' button and click on the 'PrtScrn/Sys Rq' button. Then paste into a Word document. Note: the 'Snipping Tool' for Windows 7 and Vista will also do the job.
 Websites	**Apple Mac users:** hold the command, shift and 4 buttons then click the left mouse button whilst dragging over the area you wish to copy.
	Note: If video/audio capture is required, contact the Service Centre on 1800 680 445 or the Learning Technologies Unit (see Departmental contacts) for further assistance.
 Chatrooms	Take **screen shots** *(see steps above)* and **copy information into a Word document** or **print out hard copies** of the conversations.
 Instant messaging (IM)	
 Mobile phones	**Confiscate phone but only if such action is in accordance with** Temporary removal of student property by school staff. Do not open or access the phone. Even if the student/ victim gives permission, do not delete image, text or voice messages until the incident is resolved. Likewise, do not forward the image or text to another phone as original identifying data will be replaced in the transfer process.
 Email	It is important to **keep a copy of the original email.** Do not delete the email and ask the student involved to keep a copy until otherwise advised.
	Teachers should **print a copy** and **forward the email to the principal.**

Removal of content

Online content

If inappropriate online content is not of a criminal nature, steps should still be taken to have it removed.

Student removal of content

If the identity of the student responsible is known, the quickest and easiest way to have the content removed is to request that they remove it. It should be explained to the student why the content is considered unacceptable.

Third-party removal of content

If the student responsible refuses to delete the inappropriate or offensive content or the identity of the person who posted the material is not known, then the principal, delegate, or victim must report the content to the site's service provider and ask to have it removed. Most social networking providers have a 'Report/Block this Person' or 'Report Abuse' link on the content page or the user's profile.

The majority of sites will remove any content that contravenes their terms of service/terms and conditions/ acceptable use clauses. When reporting abuse to the service provider, read their terms and conditions and advise the service provider how the content breaches those conditions.

Principals should be mindful when communicating with third party online providers, care must be taken not to breach privacy obligations under the Information Privacy Act, and section 426 of the Education (General Provisions) Act. Personal information cannot be disclosed, except in limited circumstances, such as where the student/parent consents or where required or authorised by law. Communications with third party providers should be limited to seeking removal of the content and stating how that content contravenes terms of service.

It should be noted that some service providers (and in many cases, the police) do not accept reports by third parties, only allowing the account holder to make a request for assistance.

Mobile phone content

Mobile phone texts or conversations of a criminal nature *(see Appendix 2 - Criminal offences)*, should be referred to the police. If the activity is of a non-criminal nature, mobile phone service providers usually only accept complaints from the owner of the phone. Further, most Australian mobile phone service providers will only take action after three or more 'unwelcome calls.' Actions taken can range from cancelling the offender's phone account to giving the victim a new phone number.

Refer to Appendix 4 for contact details of mobile phone providers, chat/webmail providers and social media websites.

Reporting

If the school requires assistance from the Learning Technologies Unit, contact the Service Centre and log a job for referral to the Cybersafety and Reputation Management work group.

If the incident was resolved at school level, the OneSchool Behaviour Reporting system should be completed. In the 'Details' field of the incident record, enter the words 'Cyberbullying' or 'Reputation management' at the start of this field.

Principals and teachers should be mindful of their reporting of harm obligations under the **Child Protection Act 1999** and under the Department's **Student Protection policy.**

Principals should be mindful of their reporting obligations to the Director, Ethical Standards Unit when responding to allegations of harm to a student or suspicion of harm to a student caused by an employee under the Department's **Allegations against employees in the area of student protection policy.**

a. **Report the details, management and outcome of any low level incident to the Director, Ethical Standards Unit on a SP1: Report of student harm (suitable for local resolution) form**

b. **Report particulars of any allegations of serious harm to the Director, Ethical Standards Unit on a SP2: Report of significant harm to a student as a result of actions by an employee form and not inform the employee who is the subject of the allegation, unless otherwise directed**

c. **Report to the Director, Ethical Standards Unit and notify the relevant regional/institute/statutory authority director if the alleged matter is sexual abuse or suspected sexual abuse of a student by an employee on a SP3: Report of suspected sexual abuse of a student by an employee form and not inform the employee, who is the subject of the allegation, unless otherwise directed.**

Teachers who have been subjected to cyberbullying or reputation management incidents initially may be reluctant to report them to their school principal or delegate. If they prefer, teachers can seek advice, support or report incidents by:

- submitting a job via Service Now
- contact the Department's Learning Technologies Unit for advice or support
- contact the EAS or Queensland Teacher's Union for additional support
- contact the police directly if they find comments threatening / harassing / menacing.

(see Queensland Government contacts on page 13)

Staff members (e.g. teachers and principals) can contact the police directly if they find comments threatening/harassing /menacing, e.g. threats to kill or harm people or property?

Teachers should be mindful they have an obligation under **Allegations against employees in the area of student protection policy** to immediately report to the school principal and keep appropriate records of any allegation or information about an employee suspected of causing harm to a student.

Note: the Department's Legal and Administrative Law Branch cannot provide legal advice to individual staff members (e.g. teachers) in relation to private legal matters (e.g. defamation).

Relevant policy and procedures

Code of School Behaviour
http://education.qld.gov.au/publication/production/reports/pdfs/code-school-behaviour-a4.pdf

Responsible Behaviour Plan for Students
http://education.qld.gov.au/studentservices/behaviour/bm-plans.html

Code of Conduct
http://education.qld.gov.au/corporate/codeofconduct/

Acceptable Use of the Department's Information, Communication and Technology (ICT) Network and Systems
http://ppr.det.qld.gov.au/corp/ict/management/Pages/Acceptable-Use-of-Departments-Information-Communication-and-Technology-(ICT)-Network-and-Systems.aspx

Managing Electronic Identities and Identity Management
http://ppr.det.qld.gov.au/corp/ict/management/Pages/Managing-Electronic-Identities-and-Identity-Management.aspx

Appropriate Use of Mobile Telephones and other Electronic Equipment by Students
http://ppr.det.qld.gov.au/education/learning/Pages/Appropriate-Use-of-Mobile Telephones-and-other-Electronic-Equipment-by-Students.aspx

Student Protection
http://ppr.det.qld.gov.au/education/community/Pages/Student-Protection.aspx

Safe, Supportive and Disciplined School Environment
(which includes a link to information on 'natural justice and fair and equitable practice')
http://ppr.det.qld.gov.au/education/learning/Pages/Safe,Supportive-and-Disciplined-School-Environment.aspx

Temporary removal of student property by school staff
http://ppr.det.qld.gov.au/education/management/Pages/Temporary-Removal-of-Student-Property-by-School-Staff.aspx

Allegations against employees in the area of student protection
http://ppr.det.qld.gov.au/corp/hr/management/Pages/Allegations-Against-Employees-in-the-Area-of-Student-Protection.aspx

Disclosing Student Personal Information to the Queensland Police Service
http://ppr.det.qld.gov.au/education/community/Pages/Disclosing-Student-Personal-Information-to-the-Queensland-Police-Service.aspx

Queensland Government contacts

For further information please contact:

Principal Advisor, Cybersafety and Reputation Management
Learning Technologies Unit, Web and Digital Delivery
Department of Education, Training and Employment

Phone: 07 3421 6335
Email: Cybersafety.ReputationManagement@deta.qld.gov.au

Service Centre
Department of Education, Training and Employment

Phone: 1800 680 445
Email: servicecentre@deta.qld.gov.au

Employee Assistance Service (EAS)

Contact details for your local Employee Advisor can be found by visiting: **http://education.qld.gov.au/health/employee.html**

Queensland Teacher's Union

Website: http://www.qtu.asn.au/

Appendices

Appendix 1 –Types of mobile phone and electronic communication technology incidents

The range of mobile phone and electronic communication technology incidents which may affect the good order and management of the school for the school includes:

- sending or posting abusive, threatening, harassing, humiliating or embarrassing messages about another person via text, social networking sites, websites, email or other electronic communication applications
- spreading rumours or lies about others via text, social networking sites, websites, email or other electronic communication applications
- forwarding personal emails, messages, pictures or videos to others without permission
- taking, sending or posting embarrassing, degrading or 'fight' videos involving others via text, social networking sites, websites, email or other electronic communication applications
- taking, sending or posting sexually explicit images of other children using mobile phone or web applications
- using social networking sites, websites, or blogs to post inappropriate photographs about other children or school staff
- maliciously excluding children online through emails, chat and social networking sites
- making prank calls to another child's mobile phone
- using another student's mobile phone, school MIS account, personal email account or social networking profile to send or post material which damages their social status or interaction with other children
- assuming another child's identity and creating a false email account, social networking profile or blog to send or post material which damages that child's social status or relationships with other children
- assuming a teacher's identity and creating a false email account or social networking profile to send or post material which damages the teacher's reputation
- creating a false social networking profile or website of a school to damage the reputation of the students, staff or school
- creating gossip pages on social networking sites by posting sexual, abusive, threatening, harassing, humiliating or embarrassing messages about other students.

Appendix 2 - Criminal offences

Cyberbullying and other forms of inappropriate online activity may in certain circumstances constitute a criminal offence. Both the 'Criminal Code Act 1995' (Cth) and the 'Criminal Code Act 1899' (Qld) contain relevant provisions.

The Criminal Code Act 1995 (Cth)

Part 10.6 Division 474 of the 'Commonwealth Criminal Code' outlines a number of criminal offences concerning telecommunications services. Potentially relevant offences for cyberbullying include:

- using a carriage service to make a threat to kill or seriously harm another person (s. 474.15)
- using a carriage service to menace, harass or cause offence to another person (s. 474.17)

using a carriage service to promote methods for suicide or counsel another to commit suicide (ss. 474.29A & 474.29B).

Criminal Code Act 1899 (Qld)

The Queensland Criminal Code contains several applicable sections for cyberbullying. Potential relevant criminal offences are:

- unlawful stalking (s.359E)
- possession of child exploitation material (s.228D)
- involving a child and making child exploitation material (s.228A and s.228B)
- distribution of child exploitation material (s.228C)
- criminal defamation (s.365)
- counseling, aiding or procuring suicide (s.311).

Unlawful stalking

Under the Queensland Criminal Code, chapter 33A, cyberbullying may constitute an offence of unlawful stalking.

Unlawful stalking is conduct intentionally directed at a person (the stalked person) that would cause apprehension or fear of violence to, or against property of, the stalked person or another person, or that causes detriment to the stalked person or another person (s. 359B).

For the conduct to constitute unlawful stalking it must be engaged in on any one occasion if the conduct is protracted, or on more than one occasion. It must also consist of one or more acts of the following or similar:

- following, loitering near, watching or approaching a person
- contacting a person in any way, including, for example, by telephone, mail, fax, email or through the use of any technology
- loitering near, watching, approaching or entering a place where a person lives, works or visits
- leaving offensive material where it will be found by, given to or brought to the attention of, a person (including internet posts, blogs, websites, social networking sites
- giving offensive material to a person, directly or indirectly
- an intimidating, harassing or threatening act against a person, whether or not involving violence or a threat of violence
- an act of violence, or a threat of violence, against, or against property of, anyone (s. 359B).

The maximum penalty for unlawful stalking is five years imprisonment.

continued on next page

Appendix 2 - Criminal offences (continued)

Offences involving child exploitation material

- Sections 228A to D of the Queensland Criminal Code provide offences for involving a child in the making, distributing and possessing of child exploitation material.
- The Queensland Criminal Code defines child exploitation material as material that, in a way likely to cause offence to a reasonable adult, describes or depicts someone who is, or apparently is, a child under 16 years:
- (a) in a sexual context, including for example, engaging in a sexual activity; or
- (b) in an offensive or demeaning context; or
- (c) being subjected to abuse, cruelty or torture.

The maximum penalty for the offences under s.228A, s.228B and s.228C is ten years (five years in respect of s.228D) imprisonment and possible inclusion on the Australian National Child Offender Register.

Sexting

- The act of sending, forwarding or distributing sexually explicit messages or images electronically is commonly referred to as 'sexting'. Students should be made aware that by distributing explicit (nude or semi-nude) images of themselves or other children, they may be committing a number of offences against the Queensland Criminal Code, child exploitation material provisions.

Note: school staff should be aware of their reporting of harm obligations under the Child Protection Act 1999 (Qld). *See* Student Protection.