Cyberbullying
and reputation management

Incident management guidelines for principals
## Contents

**Overview** 3

A school's approach to cyberbullying and reputation management 3

Incident management response 4

Incident management response flowchart 7

How to preserve evidence 8

Removal of content 10

Reporting 11

Relevant policy and procedures 12

Queensland Government contacts 13

Appendices 14

Appendix 1 - Types of mobile phone and electronic communication technology incidents 14

Appendix 2 - Criminal offences 15

Appendix 3 - Contacts for reporting abuse 17

Appendix 4 - Further resources 18
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 procedure 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: If the online behaviour/content raises concern of risk to students submit a ‘SP4: Report of suspected harm or risk of harm’.

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 procedures.

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 procedures (see How to preserve evidence on page 8).

If the material in question is child exploitation material the police should be notified immediately 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 procedure 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 as soon as possible 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 procedures.

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

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 may wish to provide information to 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.

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, procedure requires the principal to report the incident to the Director, Ethical Standards. For further information refer to procedures 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@dete.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)*
1. Does the online behaviour impact on the good order and management of the school.

2. Determine level of threat to student/staff safety as priority.

3. Initiate an incident response.

4. Preserve any evidence, log a job with Service Centre if assistance is required.

5. Seek advice or report/consult police

6. Take steps to have upsetting or inappropriate content removed as soon as possible.

7. Report the incident to the department.

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

9. If allegations or incident involves suspected harm to a student by an employee, report to Director, Ethical Standards in accordance with Departmental policy SMS-PR-042.

If the online behaviour raises concern of risk to students submit an ‘SP4: Report of suspected harm or risk of harm’

Is there a potential crime?

Yes  No

Yes

No
How to preserve evidence

The school should preserve any evidence of the incident, where legally permissible. As noted above, staff should not 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 and the police may need to be contacted immediately.

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.

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.

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.

Using the print to pdf tool is a recommended method of recording screens.

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.

Video hosting sites such as YouTube

Websites

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.

Note: Child exploitation material must not be saved, copied, printed or otherwise dealt with. Concerns about explicit content should be escalated to the Cybersafety and Reputation Management team.
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 2009 (Qld), and section 426 of the Education (General Provisions) Act 2006 (Qld). Personal information cannot be disclosed, except in limited circumstances 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 obligations under the Child Protection Act 1999 and under the Department’s Student Protection procedure.

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 procedure.

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 Teachers’ Union (if a member) for additional support
- contact the police directly if they find comments threatening / harassing / menacing.

(see Queensland Government contacts on page 13)

Teachers should be mindful they have an obligation under Allegations against employees in the area of student protection procedure 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

Responsible Behaviour Plan for Students

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

Acceptable Use of the Department’s Information, Communication and Technology (ICT) Network and Systems

Managing Electronic Identities and Identity Management

Appropriate Use of Mobile Telephones and other Electronic Equipment by Students

Student Protection
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’)

Temporary removal of student property by school staff
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
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
ppr.det.qld.gov.au/education/community/Pages/Disclosing-Student-Personal-Information-to-the-Queensland-Police-Service.aspx
Important incident management contacts

For further information please contact:

Manager Cybersafety and Reputation Management
Learning Technologies Unit, Web and Digital Delivery
Department of Education, Training and Employment
Phone: 07 3421 6335
Email: Cybersafety.ReputationManagement@dete.qld.gov.au

Service Centre
Department of Education, Training and Employment
Phone: 1800 680 445
Email: servicecentre@dete.qld.gov.au

Employee Assistance Service (EAS)
Contact details for your local Employee Advisor can be found by visiting:
education.qld.gov.au/health/employee.html

Queensland Teachers’ Union
Website: 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 includes:

- sending or posting abusive, threatening, harassing, humiliating or embarrassing messages about another person via text, social networking sites/apps, websites, email or other electronic communication applications
- spreading rumours or lies about others via text, social networking sites/apps, 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/apps, 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/apps, 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/staff.
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 for child pornography material (s.474.19)
- 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)
- counselling, 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.
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 and involving a child in the making 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:
  » in a sexual context, including for example, engaging in a sexual activity; or
  » in an offensive or demeaning context; or
  » being subjected to abuse, cruelty or torture.

The maximum penalty for the offences under s.228A, s.228B, s.228C and s. 228D is fourteen years 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.
### Mobile phone providers

<table>
<thead>
<tr>
<th>Provider</th>
<th>Phone Number</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optus</td>
<td>1800 780 219</td>
<td></td>
</tr>
<tr>
<td>Virgin Mobile</td>
<td>1300 555 100</td>
<td></td>
</tr>
<tr>
<td>Vodafone</td>
<td>1800 638 638</td>
<td></td>
</tr>
</tbody>
</table>


### Video hosting sites

<table>
<thead>
<tr>
<th>Provider</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>YouTube</td>
<td><a href="youtube.com/t/contact_us">youtube.com/t/contact_us</a></td>
</tr>
</tbody>
</table>

### Social networking websites

<table>
<thead>
<tr>
<th>Provider</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td><a href="facebook.com/safety">facebook.com/safety</a></td>
</tr>
<tr>
<td>Twitter</td>
<td><a href="support.twitter.com">support.twitter.com</a></td>
</tr>
<tr>
<td>Google (including YouTube)</td>
<td><a href="google.com/support/go/legal">google.com/support/go/legal</a></td>
</tr>
<tr>
<td>Instagram</td>
<td><a href="help.instagram.com/285881641526716">help.instagram.com/285881641526716</a></td>
</tr>
<tr>
<td>Tumblr</td>
<td><a href="tumblr.com/help">tumblr.com/help</a></td>
</tr>
</tbody>
</table>

### Instant Messaging services

<table>
<thead>
<tr>
<th>Provider</th>
<th>Website</th>
</tr>
</thead>
</table>

If conversation logs are required for reporting abuse, you should note that conversation logs are not turned on by default in most instant messaging programs.
Appendix 4 - Further resources

A parent fact sheet outlining methods for removal of inappropriate content and protecting student privacy will be made available on the ‘Parents and Carers’ section of the Student Services website. Further advice and assistance for schools and parents on the removal of inappropriate content can be requested from the Learning Technologies Unit.

Additional cybersafety resources are also available on the following websites:

**Department of Education, Training and Employment’s Student Services - Cybersafety**


This page is from the Department of Education, Training and Employment’s Student Services website. It provides information and resources on cybersafety for parents, teachers and students. A link is also provided on this website for installation of the ‘cybersafety button’ for home use.

**Working together: A toolkit for effective school based action against bullying**


This page is from the Department of Education, Training and Employment’s Student Services website, providing information and resources on bullying for parents, teachers and students.

**Bullying No Way!**

[bullyingnoway.gov.au](http://bullyingnoway.gov.au)

Developed and managed by all Australian education authorities for use by Australia’s Government, Catholic and Independent school communities.

**Australian Communications Media Authority (ACMA) Cybersmart program**

[cybersmart.gov.au](http://cybersmart.gov.au)

Provides activities, resources and practical advice to help young kids, teens and parents safely enjoy the online world. Cybersmart also offers training and resources for schools. Cybersmart is part of the Australian Government’s cybersmart program.

**ThinkUknow Campaign - Australian Federal Police (AFP)**

[thinkuknow.org.au](http://thinkuknow.org.au)

Provides information and resources on cybersafety to parents, carers, teachers and youth aged 11 to 17 years.

**Kids Help Line**


Kids Helpline produces content on cyberbullying for different age groups. The site contains ready-made lesson packs to help teachers educate students about cyberbullying, sexting and the safe use of technology.

**Good to Know: A guide to staying safe and secure online - Google**

[google.com/goodtoknow](http://google.com/goodtoknow)

Stay safe and secure online. Explore quick tips and how-to’s that explain what you can do to stay safe and secure on the web.

**Digital Parenting - Vodafone**

[vodafone.com/content/index/parents.html](http://vodafone.com/content/index/parents.html)

This website is an overview for parents on how to support their children with being safe online. It features ‘how to’ guides and expert videos, tailored for parents/caregivers.

**Young and Well Cooperative Research Centre**

[youngandwellcrc.org.au](http://youngandwellcrc.org.au)

The Young and Well Cooperative Research Centre is an Australian-based, international research centre that explores the role of technology in young people’s lives, and how it can be used to improve the mental health and wellbeing of young people aged 12 to 25.