# Fact sheet

# Cyberbullying and school aged students

# What is cyberbullying?

Cyberbullying is bullying conducted with the use of technology, like mobile phones or the internet.

This is the <u>national definition of bullying</u> for Australian schools.

Bullying is the ongoing and deliberate misuse of power in relationships through repeated verbal, physical and/or social behaviour that intends to cause physical, social and/or psychological harm. It can involve an individual or a group misusing their power, or perceived power, over one or more persons who feel unable to stop it from happening.

Bullying can happen in person or online, via various digital platforms and devices and it can be obvious (overt) or hidden (covert). Bullying behaviour is repeated, or has the potential to be repeated, over time (for example, through sharing of digital records).

Bullying of any form or for any reason can have immediate, medium and long-term effects on those involved, including bystanders. Single incidents and conflict or fights between equals, whether in person or online, are not defined as bullying.

# Responsibilities

All incidents that directly affect the good order and management of a school will be managed in line with the school's **Student Code of Conduct**. Principals and school staff have the same responsibility to respond to allegations of cyberbullying as they would any other incident of bullying reported.

# **Principals**

- ensure that their school's Student Code of Conduct clearly articulates the school's approach for responding to allegations of cyberbullying and includes the cyberbullying response flowchart
- ensure the school community is aware of the school's approach for responding to and managing allegations of cyberbullying
- develop individual school-based policies regarding the use of mobile phones and other technology as part of the school's Student Code of Conduct (refer to Student Code of Conduct template)
- provide clear guidance to students and parents about the appropriate use of mobiles and other electronic devices — at school and outside of school (refer to Guidance document).
- share information appropriately and as necessary with staff about any incidents of alleged cyberbullying
- where appropriate, take statutory disciplinary action to address cyberbullying:
  - that occurs outside of school hours or school grounds that
    also negatively affects the good order and management of
    the school (e.g. where the conduct, threats, intimidation
    or abuse have created, or would likely create a risk of,
    substantial disruption within the school environment, or
    where the conduct, threats, intimidation or abuse has or
    might reach school premises); OR
  - that is undertaken on or originating from school premises during school hours, or by means of use of school ICT, concerning other students, staff or members of the school community.
- use non-statutory options to deal with the matter, for example:
  - discussion with student's parents;
  - student mediation;
  - apology;

- ICT / mobile technology ban;
- guidance referral.
- must if at any point a reasonable suspicion is formed that
  a student has been harmed or is at risk of harm, respond in
  accordance with the <u>Student protection procedure</u>.
- must regardless of whether or not the cyberbullying is a
  matter that must be dealt with by the school Principal as per
  this document, support the wellbeing of any student who is
  displaying apparent negative effects from cyberbullying by
  means of offering the appropriate support.

# State school staff (including principals)

- treat cyberbullying with the same level of seriousness as other forms of bullying
- follow processes outlined in the school's Student Code of Conduct and the cyberbullying response flowchart to respond to allegations and incidents of cyberbullying
- ensure records in OneSchool are maintained accurately in relation to any allegations of cyberbullying
- support the wellbeing of any student who is displaying apparent negative effects from cyberbullying by discussing guidance officer support.
- do not open, search or otherwise deal with the property of a student (such as a mobile device) without the consent of the student or parent (refer to <u>Temporary removal of student</u> <u>property by school staff procedure</u>)
- remove property, including mobile phones, from a student
  if it is necessary to promote the caring, safe and supportive
  learning environment of the school, to maintain and foster
  mutual respect between all state school staff, students and
  visitors (refer to <u>Temporary removal of student property by</u>
  school staff procedure).

## Students must be advised:

- how to use technology appropriately
- to make a report about cyberbullying by approaching a familiar or trusted teacher
- that if they engage in cyberbullying they will likely face statutory or non-statutory disciplinary action
- if they have concerns about cyberbullying incidents that occur outside of school hours, including weekends or school holidays that they should immediately seek assistance through the <u>Office of the eSafety Commissioner</u> or the <u>Queensland Police Service</u>
- if they are suffering negative effects from cyberbullying that they can seek guidance support from the school or other support services such as headspace or Kids Helpline.

## Resources

- Online incident management guidelines for school leaders
- Cybersafety in Queensland state schools
- Supporting students' mental health and wellbeing procedure
- <u>Temporary removal of student property by school staff procedure</u>
- Bullying. No Way!
- Kids Helpline
- headspace
- Be You



# How to manage online incidents that impact your school

#### Student protection

If at any point the principal forms a reasonable suspicion that a student has been harmed or is at risk of harm, they have a responsibility to respond in accordance with the <a href="Student protection procedure">Student protection procedure</a>.

## **Explicit images**

If the investigation involves naked or explicit images of children, staff should not save, copy, forward or otherwise deal with the content, as per the <a href="Temporary removal of student property by school staff procedure">This includes onto OneSchool records</a>. Refer to the investigative process outlined in 'Responding to incidents involving naked or explicit images of children' from the <a href="Online Incident management guidelines">Online Incident management guidelines</a>.

#### Report

Refer to the Online incident management guildelines for more details or, if assistance is required, submit a request to remove harmful online content through the Services Catalogue Online. For further support, contact the Cybersafety and Reputation Management team on 3034 5035 or email Cybersafety@qed.qld.gov.au.

# Does the online behaviour/incident negatively impact the good order and management of the school?



#### 1. Initiate an incident response

Start an incident management log (running sheet) which records times and dates of events, observations, tasks completed, persons involved and written conversational notes.

#### 2. Collect evidence

Gather and preserve any <u>evidence</u> of the online content or a potential unlawful online behaviour, where legally permissible. Confiscation of digital devices can only be done under the <u>Temporary removal of student property by school staff</u> procedure.

#### 3. Is there a potential crime?

The  $\underline{\text{Queensland Criminal Code}}$  contains several applicable sections for cyberbullying. A list of potential relevant criminal offences can be viewed at  $\underline{\text{Appendix 3}}$ , and include:

- unlawful stalking
- computer hacking and misuse
- possession, distribution and making child exploitation material
- fraud obtaining or dealing with identification information
- criminal defamation.

Inform the student's parent/s (and student if appropriate) of their options:

- Report the incident to an external agency such as police, <u>Office of</u> the <u>eSafety Commissioner</u> or the <u>Australian Cybercrime Online</u> <u>Reporting Network</u>.
- Report the online content/behaviour using the online tools provided by the website or app.

Principals may start contact with a law enforcement agency (LEA) by completing an LEA referral form, under the <u>Disclosing personal information to law enforcement agencies</u> procedure. Refer back to Step 3 to report potential crimes that do not negatively impact the good order of the school.

NO



Principals may start contact with a law enforcement agency (LEA) by completing an <u>LEA referral form</u>. Information can be shared when reasonably satisfied the disclosure is necessary for the prevention, detection, investigation, prosecution or punishment of a criminal offence or to assist in averting a serious risk to the life, health or safety of a person or where the disclosure is in the public interest. For access to the relevant forms, refer to <u>Disclosing personal information to law enforcement agencies</u> procedure.

Principals may continue to investigate the matter for disciplinary purposes, subject to all laws and department procedures.

Content may not constitute a criminal offence requiring police involvement but it may negatively impact the good order and management of the school. Principals can take action for the online behaviour as outlined below.

#### 4. Take steps to remove the upsetting or inappropriate content

Request poster to remove, use online reporting tools or if assistance is required, contact the CSRM team or Office of eSafety Commissioner.

### 5. Managing student behaviour

Where the online behaviours of students do negatively impact the good order and management of the school, the principal must take appropriate follow-up action. Where appropriate:

- take statutory disciplinary action to address cyberbullying:
  - that occurs outside of school hours or school grounds that also negatively affects
    the good order and management of the school (e.g. where the conduct, threats,
    intimidation or abuse have created, or would likely create a risk of, substantial
    disruption within the school environment, or where the conduct, threats,
    intimidation or abuse has or might reach school premises);
  - that is undertaken on or originating from school premises during school hours, or by means of use of school ICT, concerning other students, staff or members of the school community:

# **OR** • use non-statutory options to deal with the matter, for example:

- discussion with student's parents;
- student mediation;
- apology;
- ICT / mobile technology ban;
- guidance referral.

# 6. Student welfare

Principals must consider and support the wellbeing of any student who is displaying apparent negative effects from cyberbullying, by means of offering the student guidance officer support.

#### Recording the incident on OneSchool

If the incident was resolved at school-level, record details of the incident, as reported to the school and investigated through the incident management process, in the student's OneSchool behaviour record.

