

Cyber Safety

Policy framework for schools and systems

1. General Principles

1.1 Definitions

Ensuring cyber safety involves the active promotion of cyber safe behaviours based on the safe, respectful and responsible use of internet and mobile phone technologies, and the taking of specific measures to remove the risks of any inappropriate and harmful use of these technologies.

In an education setting, cyber bullying refers to the deliberate and repeated misuse of technology to harass, threaten, insult or ridicule students or staff. Examples include threatening texts, emails or instant messages, online denigration, vilification or defamation, derogatory websites, disturbing private pictures or videos, and online exclusion or impersonation. In schools and other education settings, victims of cyber bullying include both students and staff.

1.2 Schools Duty of Care to Students and Staff

Despite the potential for serious consequences, there is no Australian law that deals specifically with cyber bullying. There are, however, a number of laws which have a related impact on the duty of care of schools.

Schools hold a duty of care to students and staff and are required under various legislative frameworks, including OHS and Injury Compensation legislation, to ensure that the environment in which staff and students work is free from risk of harm. Schools can be sued for damages for not intervening in severe cases of bullying. The civil law of negligence imposes a duty of care on school authorities to take reasonable precautions to prevent both physical and psychiatric harm in circumstances where the teacher-student relationship exists.

In some cases, courts have held that this relationship may extend beyond school gates and hours.

1.3 Policies and procedures

Effective and proactive procedures and practices for

both preventing and dealing with cyber bullying are a key part of comprehensive intervention strategies to address bullying. Current research shows that the presence of formal whole school anti-bullying policy is an effective component of bullying prevention programs. A key resource for schools is the National Safe Schools Framework.

Such policies are emerging as effective strategies for reducing cyber bullying. However, because of the technological context of cyber bullying, there is a need to develop and implement specific strategies such as cyber safety education and promoting the positive uses of technology.

Effective cyber safety measures should be integrated into school's current policies and practices, including those dealing with ICT use, anti-bullying, harassment and discrimination. These measures need to be multi-disciplinary, whole school interventions and be integrated into student education programs and be the focus of specific staff training.

The development and dissemination of policies and procedures with:

- clear codes of conduct
- statements of the specific rights, responsibilities and obligations of school authorities, staff, students and parents
- clear and accessible reporting mechanisms, complaints handling procedures, and links to the school's discipline policies should assist the school to meet its obligations of duty of care to students and staff.

1.4 Consultation and on-going involvement

It is important to develop clear policies in conjunction with and for students, staff and parents in respect to the positive and expected use of information technology. This helps to ensure clarity and consistency for all members of the school community.

Schools should have a broadly representative advisory committee that oversees the development, implementation and monitoring of cyber safety and ICT

related matters including cyber bullying, appropriate ICT use and related educational programs and training. This committee should have clear links with other key school committees such as Human Resources and Curriculum committees.

Part of the development and implementation of policies and procedures is the necessity to ensure a common understanding of bullying, including cyber bullying, definitions, negative effects, moral and legal aspects. Also important is the promotion and implementation of proactive measures to ensure that staff, students and families are recognising, monitoring and responding in consistent ways to this behaviour.

Therefore clear strategies focusing on communication and on-going education of students, parents and staff must be part of a school's formal policy and its policy implementation strategies.

It is essential to also involve the school's IT professionals to ensure that policy and practices are inextricably linked to schools' use of ICT, such as via a student laptop program. Creating links with IT services may be relevant for cyber bullying, because of the technical challenges posed, such as the use of preventive strategies that require specific cyber safety knowledge, and the removal of harmful or defamatory content on websites, as well as how to retain evidence of cyber bullying.

2. Policy Framework

This IEU Policy Framework aims to assist in the development and implementation of effective school policy that will guide and protect both staff and students.

2.1 Develop Clear and Integrated Policies

- Include definitions and glossary using clear plain language, including definitions of student wellbeing, aggression, violence, bullying, cyber bullying, cyber harassment and acceptable use of technology
- Summarise existing legislation that may be called upon, including OHS legislation, Hate/Vilification laws, Discrimination/Sexual or Racial harassment law, Privacy law, Defamation law, Telecommunications Offences under the Australian Commonwealth Criminal Code Act 1995, Stalking legislation (for example recent amendments to include bullying in the Stalking Interventions Act Vict).
- Include information about :
 - the school's expectations about student's positive behaviour toward others in the school including when outside school hours and off school grounds
 - all school community members' rights to and responsibilities for safety and wellbeing

- the school's role in managing any behaviours that occur that are not consistent with the school policy
- Include a code of conduct for use of ICT including a Cyber-Safety Use Agreement Form relevant for:
 - students
 - teachers/support staff
 - parents/volunteers using school ICT equipment.
- Outline the make up of a cyber safety committee at your school that revises the policy at regular intervals or when necessary
- Demonstrate links to existing policies/procedures in the school, for example, discipline or bullying policies, other complaint handling procedures
- Demonstrated links to other ICT policies such as acceptable use of email.

2.2 General Procedures

- Outline how online safety/bullying incidents are to be reported by
 - teachers/support staff
 - students
 - parents/caregivers
- Differentiate and outline the procedures for responding to incidents as appropriate, including procedures for dealing with critical incidents that impact on the effective operation of the school or create a danger or risk to individuals at the school or on school related activities (i.e. a critical incident policy)
- Show a clear chain of authority for each type of incident
- Outline a method of tracking issues/incidents to ensure timely responses
- Include procedures for managing media, if this becomes applicable
- Outline procedures for providing parental access to records about their children
- Include a timeline for revision of policy
- Commit to testing the policy annually against hypothetical incidents drawn from media stories at the time. This will help the policy remain up to date with:
 - developments in technology/the population's use of technology
 - changes in legislation or new precedents set by courts.

2.3 Responding to incidents

- Show a clear difference between discipline and counselling actions as appropriate to the incident
- Outline appropriate initial responses to a complaint to the:
 - target of incident (be it student/parents/teacher/support staff/outside school community member)
 - alleged perpetrators (be it a student/parent/teacher/support staff/outside school community

- member)
- Create appropriate response procedures for different types of incidents:
 - outline who is responsible and able to respond for different types of cases
 - show where the police or government agency may/must become involved.
 - show when to involve parents
- Make a clear reference as to how and when the school's discipline policy will be engaged.

2.4 *Communication of policy to the school community*

- Make sure that your school is providing clear and consistent advice about what is expected and acceptable to:
 - teachers/support staff
 - parents/caregivers/community volunteers
 - students.

2.5 *Professional development of teachers and support staff*

- Make sure all school staff receive professional development about:
 - their legal rights and responsibilities
 - what the policy covers
 - how and when to apply the policy
 - the development and delivery of education programs related to implementation of the policy.

2.6 *Education of parents/caregivers/volunteers*

- Communicate and educate regularly in a variety of ways, for example:
 - involve parents in policy review committee
 - regular information nights - not just for parents of students entering the school
 - have guest speakers, for example:
 - police
 - Australian Communication and Media Authority (www.cybersmart.gov.au)
 - www.thinkuknow.org.au (Australian Federal Police in association with Microsoft and others]
 - former targets of bullying
 - university lecturers
 - a student drama presentation/short film
 - supply printed and online materials in various ways, for example:
 - regular column in newsletters
 - information pamphlet
 - yearly school magazine reports on activities of student populace to increase cyberspace safety awareness.

2.7 *Education of students*

- Make the elements of the policy an integrated part of your school culture in various ways, for example:

- ensuring consistency in staff and student understanding and application of behaviour protocols
- integrating it into existing units of study so that students' understanding and skills involved in cyber safety, countering harassment, aggression, violence and bullying develop in age appropriate and relevant ways
- using www.cybersmart.gov.au and www.thinkuknow.org.au resources
- involving students in a policy creation committee
- getting students to educate and inform student body and parents through:
 - drama presentations
 - student-run forums for parents
 - columns in newsletters/school magazine.

3. Resources

The National Safe Schools Framework - Resource Manual (www.safeschools.deewr.gov.au) provides a very comprehensive list of websites for the applicable legislation, resources and organisations at both the national and state level.

4. Other IEU related policies for reference

Internet and Email Use
 Workplace Bullying
 Personal Files
 IEU Privacy Policy
 Handling Complaints Against Staff
 Managing Violence in Schools
 Anti Racism

Endorsed by the Annual Conference of IEU Victoria Tasmania November 2011