



Guidelines for Administrators to Address Cyber Bullying

What steps should school administrators take to protect students from cyber bullying? The following approaches are recommended (Kowalski, Limber, and Agatston 2008):

1. Develop rules and policies that prohibit the use of district computers and other cyber technologies at school to bully or harass others.

These can be incorporated into existing policies that address acceptable uses of technology by students (often termed “acceptable use policies”). Or administrators may address cyber bullying through policies that specifically focus on bullying. The following elements of a good policy are included on pages 49–50 in the Schoolwide Guide for the *Olweus Bullying Prevention Program*:

- a clear definition of bullying
- a focus on prevention
- the use of *OBPP*’s Four Anti-Bullying Rules
- the use of negative consequences for bullying and positive consequences for prosocial behavior or active bystander efforts
- procedures for reporting bullying, including the process for reporting and responding
- procedures for intervening and addressing bullying as it occurs and when it is reported

- procedures for working with parents and guardians when bullying problems occur
- district-level standards for logical consequences and disciplinary actions
- district-level policies for handling disputes and incidents that cross the line into illegal behaviors such as assault, sexual harassment, disability harassment, hazing, and discrimination

For guidance on the development of an acceptable use policy, administrators may view the Model Acceptable Use Policy for Information Technology Resources in the Schools (U.S. Department of Justice) as a starting point. This model policy requires, in part, that students comply with these rules:

- Respect and practice the principles of community.
- Communicate only in ways that are kind and respectful.
- Report threatening or upsetting materials to a teacher.
- Do not intentionally access, transmit, copy, or create material that violates the school's code of conduct, for example, messages that are pornographic, threatening, rude, discriminatory, or meant to harass.
- Do not intentionally access, transmit, copy, or create material that is illegal, such as obscenity, stolen materials, or illegal copies of copyrighted works.
- Do not use the resources to further other acts that are criminal or violate the school's code of conduct.
- Do not send spam, chain letters, or other mass unsolicited mailings.
- Do not buy, sell, advertise, or otherwise conduct business, unless approved as a school project.

Because *bullying* and *harassment* have different legal connotations, it is recommended that even more specific language be included under the fourth point: "Do not intentionally access, transmit, copy, or create material that violates the school's code of conduct, such as messages that are pornographic, threatening, rude, discriminatory, or meant to

bully or harass.” A complete copy of the model policy may be found at www.usdoj.gov/criminal/cybercrime/rules/acceptableUsePolicy.htm.

2. Establish policies and procedures that limit students’ use of school Internet resources to academic purposes only.

Under the U.S. Department of Justice model policy just mentioned, if students are in compliance with the policy, they may do the following:

- Design and post Web pages and other material from school resources
 - Use direct communications, such as Internet Relay Chat (IRC), online chat, or instant messaging, with a teacher’s permission
 - Install or download software, if also in agreement with laws and licenses, and under the supervision of a teacher
 - Use the resources for any educational purpose
3. Educate faculty, staff, students, and parents and guardians about cyber bullying and the school’s policies and procedures.

It is not necessary for all faculty and staff members to be trained as experts on cyber bullying, but they should be familiar with the issue and know how to recognize and to respond to cyber bullying if students raise concerns. In addition, certain staff members (for example, counselors, administrators, media specialists) should have specific training to address cases of cyber bullying that may surface (Kowalski, Limber, and Agatston 2008). A Teacher Training Presentation on this CD-ROM provides basic information for faculty and staff about cyber bullying.



School districts should provide copies of any cyber bullying policy to faculty, staff, parents and guardians, and students.

4. Provide adequate supervision and monitoring of students, including their use of the Internet.

Bullying thrives where adults are not present or not observant. Students’ behavior at school should be monitored closely for signs of possible bullying or misuse of technology, for example, the use of cell phones on campus. Students’ use of computers in classrooms should be closely

monitored, and school staff members should routinely inspect school computers and students' Internet accounts.

5. Establish a schoolwide reporting system for students, faculty, staff, and parents and guardians to report suspected cyber bullying or other misuse of cyber technologies.

This will encourage students to report instances of bullying that they are aware of or suspect. Some schools have created forms that students and/or staff may complete to report bullying, including a description of the incident and the location where it occurred, which could be a Web address. For an example, see the Sample Middle School Bullying/Cyber Bullying Report Form on this CD-ROM.



6. Establish effective procedures to respond to these reports.

All reports should be taken seriously and investigated thoroughly and in a timely manner. (See also Gathering Cyber Bullying Evidence on this CD-ROM.) School staff members should carefully document investigations and responses to suspected or known cyber bullying.



Reference

Kowalski, R. M., S. P. Limber, and P. W. Agatston. 2008. *Cyber bullying: Bullying in the digital age*. Malden, MA: Blackwell Publishing.