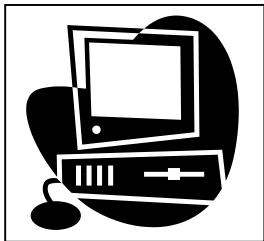


Cyberbullying or Cyberthreat Situation Review Process

- Review Team Members**
- Administrator
 - School counselor or psychologist
 - Technology coordinator
 - Librarian
 - School resource officer
 - Community mental health resource
 - Key district/regional resource
- Entire team may not be needed in all cases.



Online Incident

If the online material appears to present a legitimate imminent threat of violence and danger to others, contact law enforcement, and initiate a protective response.

BUT continue with the following evidence gathering and preservation steps.

Evidence Gathering and Preservation

Step 1. Preserve the Evidence

- Preserve any evidence on district Internet system.
- Advise parents/student/staff to preserve evidence on home computer/device.
 - Offer technical assistance, if necessary.

Step 2. Seek to Identify Creator(s)

Responsibility: Technology coordinator.

- May be obvious, anonymous, or impersonation.
- Identification may not be immediately possible.
- Offer technical assistance to parents/staff.
- If anonymous cyberbully or concerns of impersonation, and there are reasons to suspect certain student(s), conduct a search of Internet use records of student(s).
- If criminal action is involved, law enforcement has significantly greater abilities to identify anonymous creators.

Step 3. Search for Additional Material

Responsibility: Technology Coordinator and Librarian.

- Search should include all suspected participants.
 - Conduct search of files and Internet use records through district Internet system (even if it appears to be off-campus activity).
 - Conduct an additional search including
 - Online environment where initial material appeared.
 - Search engine search for name and persona of student, friends, enemies, school name.
 - Online communities used by students in school.
- Highly recommend this step be taken in the context of **any** threat assessment process!

Center for Safe and Responsible Internet Use
 Website: <http://cyberbully.org> and <http://csriu.org>
 Email: info@csriu.org
 © 2005 CSRIU

Violence or Suicide Risk Assessment

- Does the evidence gathered raise concerns that student(s) may pose a risk of harm to others or self?
 - Recognize that the threat of violence or suicide may come from student(s) who posted the material or from student(s) who were victimized.
- Conduct violence or suicide risk assessment in accord with district process.

Cyberbullying Assessment

Step 1. Determine if School Can Respond Directly

- Is there a school “nexus?”
- Is there a material and substantial threat of disruption?

Step 2a. Evaluate speech directed at staff or school

Determine the nature of the material.

- Nuisance activity → Ignore it.
- Legitimate protest speech → Fully protected speech. Learn from it.
- “Put down” material, targeting teacher for perceived “negative” feature → If school nexus, respond. If no school nexus, support teacher in responding.
- “Get back at” material, angry retaliation against teacher → Must determine why student is retaliating and address overall concerns.

Step 2b. Evaluate material directed at student(s)

Must get to “root cause” understanding of relationship between students.

- “Put down” material → Possible continuation of in-school bullying.
- “Get back at” material → Possible retaliation for in-school bullying or other cyberbullying.

Determine Response Options
(See page 2)

School and Parent Action Options

School "Nexus"

If there is a school "nexus" and substantial harm, the school can impose formal discipline.

- But do not simply impose a formal disciplinary response and expect the situation to be resolved. Get to the root!
- Other actions by the school or by the parent, target, or staff member may be necessary.

No School "Nexus"

If there is no school "nexus," provide support to the target and parents, and seek an informal resolution with cyberbully and parents.

- School officials can help the parents or the target figure out the most appropriate response(s) and provide a range of assistance in following through, including technical support.
- The school counselor or school security officer can seek an informal resolution with the parents of the cyberbully. The cyberbully's parents may be totally unaware, concerned to find that their child has engaged in this kind of activity, and get the cyberbullying to stop. Or they could be very defensive. Send the cyberbully's parents a letter that includes the downloaded material and requests a meeting to address these concerns. It may be best to start with a school counselor initiated attempt at resolution and then shift to involving the school resource officer if the parents are not responsive.
- All staff should be informed about the cyberbullying and advised to report any negative incidents of in-school bullying between the participants, even very mild negative interactions, because this can establish a school nexus.
- School counselor should provide ongoing support to the target. The counseling support should address the harm and seek to empower the target with effective skills to prevent and respond to bullying, including...
 - Develop his or her personal guidelines for online involvement.
 - Make a realistic evaluation of the quality of the online community and the benefits of remaining in or leaving.
 - Recognize the need to leave an online situation that has gotten out of control.
 - Conduct a self-assessment of his or her behavior or communications that may be contributing to victimization.
 - Learn how to respond in an assertive, but not aggressive, way to any harmful communications.
 - Know when and how to gain assistance from an adult.

Parent, Target, or Staff Member Action Options

Tell the Cyberbully to Stop

- Send the cyberbully a non-emotional, assertive message telling the cyberbully to stop.

Ignore the Cyberbully

- Block or filter all further communications through email and IM contact list.
- Avoid going to the site or group where the attacks have occurred.
- Change email address, account, username, or phone number.

File a Complaint

Cyberbullying is a violation of the "Terms of Use" of most web sites, ISPs, and cell phone companies. File a complaint by providing the harmful messages or a link to the harmful material and ask that the account be terminated and any harmful material removed.

- If the cyberbully is using email, contact the ISP of the cyberbully (determine the ISP from the email address), contact the company at <support@<ISP> or look on the ISP's site for a "Contact Us" email address.
- If the material appears on a third-party web site (e.g. <http://www.webhostname.com/~kid'sname.html>) go to site's home page, file a complaint through the "Contact Us" email address.
- If the material is on a web site with its own domain name (e.g. http://www.xyzkid.com), go to Whois (http://www.whois.net) to find the owner of the site and the host company. Go to the host company's web site and file a complaint through the "Contact Us" email address.
- If the cyberbully is using a cell phone, trace the number and contact the phone company.

Be sure to save all of the communications.

One problem is the cyberbully can set up a new account.

Contact the Cyberbully's Parents

The target's parents can send the cyberbully's parents a letter that includes the downloaded material and requests that the cyberbullying stop and all harmful material be removed.

Contact an Attorney or File a Small Claims Action

An attorney can send a letter to the cyberbully's parents demanding that the cyberbullying stop. An attorney can also help file a lawsuit or help the parents file a small claims action against the cyberbully's parents for financial damages and a requirement that the cyberbullying stop.

Contact the Police

If the cyberbullying appears to be a crime, contact the police. Cyberbullying that involves threats of violence, coercion, obscene or harassing text messages, harassment or stalking, hate or bias crimes, creating or sending sexually explicit picture, sexual exploitation, or taking a picture of someone in private place could be a crime.