Cyberbullying or Cyberthreat Situation Review Process

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 steps.

Evidence Gathering

Step 1. Preserve the Evidence
- Preserve all evidence from district Internet system.
- Advise parents/student/staff to preserve evidence on home computer. Offer technical assistance.

Step 2. Seek to Identify Creator(s)
- May be obvious, anonymous, or impersonation. Identification may not be immediately possible.
- Offer technical assistance to parents/staff.
- If anonymous or concerns of impersonation, and reasons to suspect certain student(s), conduct a search of Internet use records of student(s).
- If criminal action, contact law enforcement.

Step 3. Search for Additional Material
- All suspected participants.
- Search all files and Internet use records through district system (even if it appears to be off-campus activity).
- Conduct additional search including:
  - Site where initial material appeared.
  - Search engine search for name and username(s) 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! Search for additional material may lead to evidence of legitimate, imminent threat.

Review Team Members
- Administrator
- Counselor/psychologist
- Technology coordinator
- Librarian
- Resource officer
- Community mental health
- Key regional resource
- Entire team may not be needed.

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.

Cyberbullying Assessment

Step 1. Ask if School Can Respond Directly?
- Is there a school “nexus?”
- Is there substantial threat of disruption?

Step 2A. Evaluate material directed at student(s)
- Must get to “root cause” understanding of the relationships and issues.
  - “Put down” material → Continuation of in-school bullying.
  - “Get back at” material → Retaliation for in-school bullying or other cyberbullying.

Step 2B. Evaluate material directed at staff or school
- Determine the nature of the material.
  - Nuisance activity → Ignore it or seek to have it removed.
  - 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 → Remove speech, but must determine why student is retaliating and address underlying concerns.
School Actions and Options

**Formal Disciplinary Action**
Can impose formal disciplinary response if have established a school nexus and substantial and material disruption. But still need to address:
- Removal of materials and potential of retaliation by student or online “buddies.”
- If “put down” cyberbully stop all in-school bullying. If “get back at” cyberbully, stop all in-school victimization.
- Support needs of target.

If cannot impose formal discipline, other action options still available.

**Working With Parents**

**Child who is “Put Down” Cyberbully**

**Assumptions**
- Parents unaware, but actions are against family values.
- Initial response will be disbelief, followed by anger and humiliation.
- Parents naïve about strategies to manage Internet use.

**Process**
- Send downloaded material and Parent’s Guide to parents via certified mail.
- Request meeting following day.
- Seek parental commitment to:
  - Establish prohibitions.
  - Prevent retaliation.
  - Install and use monitoring software.
  - Limit student’s access through other venues.

*Increased potential for financial liability through civil litigation is a strong leverage.*

**Child who is Target, “Get Back At” Cyberbully, or Who Has Posted Distressing Material**

**Assumptions**
- Parent could approach school or school could find out from other source.
- Initial response of parents will be significant concern for safety and well-being of child.
- If contacting parent about reported concern, establish preliminary plan of action for support prior to meeting with parents.
- If working with parent of “get back at” cyberbully or student who has posted distressing material:
  - Ensure material is removed.
  - Install and use monitoring software.
  - Address underlying bullying or emotional concerns.
- If working with parents of target:
  - Explain limitations on formal response.
  - Use appropriate Response Options to stop/remove harmful material.
  - Warn to watch for retaliation.

**Working with Students**

**Working with Student Who is Target**

**Addiction**
- Address concerns of addiction to harmful online community.
  - Convince target to leave community.
  - Find way to get the cyberbullying to stop within the community.

**Online Bully-Proofing**
- Communications are preserved, so student and counselor can evaluate and determine patterns of communication that may be precipitating bullying.
- Impact of harmful communication is invisible if target does not immediately respond.
- Delay in communications can provide opportunity for target to calm down and respond with strength.

**When to Ask for Help**
Encourage students to tell an adult if:
- They are really upset and not sure what to do.
- The cyberbullying could be a crime.
- Any cyberbullying is or might be through the Internet of cell phone at school.
- They are being bullied by the same person at school.
- The cyberbully is anonymous.
- The cyberbully is bullying other teens who may be more vulnerable.

**Parent/Student/Staff Response Options**
- Challenge the cyberbully to stop.
- Ignore the cyberbully.
- File a complaint.
- Have the parents contact the cyberbully’s parents.
- Contact an attorney.
- Contact the police.

Center for Safe and Responsible Internet Use
http://cyberbully.org
© 2006 CRSIU
May be reproduced and distributed for non-profit purposes.
Cyberbullying or Cyberthreat Situation Review Process

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 steps.

Evidence Gathering

Step 1. Preserve the Evidence
- Preserve all evidence from district Internet system.
- Advise parents/student/staff to preserve evidence on home computer. Offer technical assistance.

Step 2. Seek to Identify Creator(s)
- May be obvious, anonymous, or impersonation. Identification may not be immediately possible.
- Offer technical assistance to parents/staff.
- If anonymous or concerns of impersonation, and reasons to suspect certain student(s), conduct a search of Internet use records of student(s).
- If criminal action, contact law enforcement.

Step 3. Search for Additional Material
- All suspected participants.
- Search all files and Internet use records through district system (even if it appears to be off-campus activity).
- Conduct additional search including:
  - Site where initial material appeared.
  - Search engine search for name and username(s) 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! Search for additional material may lead to evidence of legitimate, imminent threat.

Review Team Members
- Administrator
- Counselor/psychologist
- Technology coordinator
- Librarian
- Resource officer
- Community mental health
- Key regional resource
- Entire team may not be needed.

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.

Cyberbullying Assessment

Step 1. Ask if School Can Respond Directly?
- Is there a school “nexus”?
- Is there substantial threat of disruption?

Step 2A. Evaluate material directed at student(s)
Must get to “root cause” understanding of the relationships and issues.
- “Put down” material → Continuation of in-school bullying.
- “Get back at” material → Retaliation for in-school bullying or other cyberbullying.

Step 2B. Evaluate material directed at staff or school
Determine the nature of the material.
- Nuisance activity → Ignore it or seek to have it removed.
- 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 → Remove speech, but must determine why student is retaliating and address underlying concerns.