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.

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

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.

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.
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.