Cyber Safety Considerations for K-12 Schools and School Districts

The Internet allows for access to information 24 hours a day, 7 days a week. For schools (public and nonpublic), online capabilities not only create entrée to a vast amount of resources but also facilitate distance learning and collaboration between classes and students in different locations.[1] Along with the benefits the Internet brings, however, come costs such as new threats to students. Recent news articles provide examples of these threats: One man extorted sexually explicit images from minors using social media,[i] and instances of cyberbullying have reportedly soared in New York City schools.[ii] These incidents can lead to depression and anxiety, health complaints, and decreased academic achievement by students.[iii]

Some protections for children online are provided by Federal law and regulations, such as the Children's Internet Protection Act (CIPA).[iv] CIPA aims to protect children from obscene or harmful content on the Internet. Schools or libraries that are eligible to receive discounts for telecommunications, Internet access, or internal connections through the E-rate program (Universal Service Program for Schools and Libraries) must certify they have an Internet safety policy that blocks or filters access to pictures that are obscene, child pornography, or harmful to minors.

While CIPA may help prevent students from accessing inappropriate content on the Internet, this will not protect students from the full range of online threats. To help address these, information is provided below on the most common online threats facing students and what schools can do before, during, and after an incident.

CYBER SAFETY AND CYBERSECURITY

Cyber threats can impact either the human (students, teachers, and staff) or the physical or virtual (e.g., information technology [IT] networks and systems) elements of schools and school districts. While there may be some overlap in addressing human versus physical/virtual threats, preparing for each type can require input from different individuals with experience or expertise on that topic and unique actions before, during, and after an incident. Schools may therefore choose to plan for these threats separately, but still under a broader umbrella of cyber threats.

This fact sheet focuses on addressing threats to **people in the school community**—also called ***cyber safety*** considerations. Another fact sheet addressing threats to the school's or school district's network and systems, called cybersecurity, can be found on the REMS TA Center's Website.

[1] *School* refers to all types, including private and public, and all grade levels for the purposes of this fact sheet.

Online Threats to Students

As well as the threats that all users face when going online, such as computer viruses and email scams, students are at risk from the following:

- Cyberbullying. Cyberbullying is bullying that takes place over digital devices such as cell phones, computers, and tablets. Cyberbullying can occur through SMS, text, and mobile applications (apps) or online in social media, forums, or gaming where people can view, participate in, or share content. Cyberbullying includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can include sharing personal or private information about someone else, causing embarrassment or humiliation. Some cyberbullying crosses the line into unlawful or criminal behavior.

Most common places where cyberbullying occurs:

- Social media, such as Facebook, Instagram, Snapchat, and Twitter
- SMS (Short Message Service), also known as Text Message, sent through devices
- Instant Message (via devices, email provider services, apps, and social media messaging features)
- Email

- Inappropriate Content. Adolescents and children can unintentionally come into contact with inappropriate content, such as sexually explicit material. Unsolicited obscene materials can also be received electronically.
- Sexting. Sexting is the sharing and receiving of sexually explicit messages and nude or partially nude images via text messages or apps. Sexting, while commonly occurring off school grounds, also occurs on school property, with content being sent and viewed on cell phones. Of note is that possession of sexually explicit photos received by sexting can be considered a type of possession of child pornography from a legal perspective.
- Sextortion/Ransomware. Students may also become victim to sextortion, possibly via ransomware, if they engage in sexting. Sextortion occurs when someone threatens to distribute private and sensitive material if not provided with images of a sexual nature, sexual favors, or money. Ransomware is a particular form of computer malware in which perpetrators encrypt users' files, then demand the payment of a ransom for users to regain access to their data. Ransomware can also include an element of extortion, in which the perpetrator threatens to publish data or (possibly sexually explicit) images if the victim does not do what the perpetrator wants, such as provide nude photos.

- Oversharing. Personal information that is sometimes shared by students includes their name, age, address, phone number, and Social Security number.
- Online Predation. Online predators put victims through "the grooming process," a series of steps by which they build the victim's trust by sympathizing with him or her or feigning common interests, after which they proceed to set up a face-to-face meeting with the victim and then move forward with manipulation and seduction.

Preparing for Online Threats to Students

Before an Incident

Schools and school districts can implement several cyber policies and procedures to help keep their students safe from online threats. These include the creation and implementation of responsible use policies to ensure that students are aware of appropriate online behavior, the use of filtering and blocking software at school to prevent access to inappropriate content, and education about the risks of being online and how to stay safe.

Responsible Use Policies (RUPs)

Schools and school districts are encouraged to develop an RUP, also known as an Acceptable Use Policy, before students are allowed to access the Internet at school via a school device or the student's personal device. An RUP is an agreement written in simple and accessible language among parents or guardians, students, and school personnel that outlines the terms of responsible use and consequences for misuse. Families are usually expected to acknowledge that their child(ren) will follow basic guidelines, and students agree to the standards laid out in the policy. RUPs can cover issues such as expectations for online behavior, what resources can be accessed, academic integrity when using technology, and how student data and information will be used by the school. For example, the New York City Department of Education's Internet Acceptable Use and Safety Policy provides a summary of the policy—including a hyperlink to an easy-to-read description for parents/guardians, teachers, and students—and principles for use, such as monitoring, privacy, prohibited uses of the Internet systems, and filtering, among others.[v]

Filtering and Blocking Content

One of the first ways to prevent students from accessing inappropriate content—either deliberately or accidentally—is for schools and school districts to use filtering and blocking

software, which allows users access to only preapproved Websites. Teachers and staff can help determine what sites should be blocked. Regular audits can also be conducted to ensure that appropriate online educational material can still be accessed and to determine if blocked sites should remain blocked.

Digital Citizenship

Schools and school districts are also encouraged to teach students what it means to be a responsible digital citizen as part of a broader strategy of promoting a positive school climate. A digital citizenship curriculum can include topics such as privacy and security, relationships and communication, cyberbullying and digital drama, digital footprints and reputation, self-image and identity, information literacy, and creative credit and copyright.

As an example of a digital citizenship curriculum used by the K-12 school community, the Jurupa Unified School District educates students in Internet safety, privacy, relationships, cyberbullying, self-image, copyright rules, and other topics.[vi] Lessons are age appropriate, and discussions change depending on the latest digital trends and include topics such as the importance of making only constructive comments online.

Education and Training

Students, teachers, staff, and families can also be educated on online safety. Three sources of information are the following:

1. Stop.Think.Connect. Campaign (https://www.dhs.gov/stopthinkconnect; U.S. Department of Homeland Security) is a national awareness campaign that provides resources such as videos, a toolkit, and blogs to help raise the awareness of cyber threats and how to be safer online.
2. NetSmartz® Worskhop (https://www.netsmartz.org/; National Center for Missing and Exploited Children® [NCMEC]) provides resources for parents and guardians, educators, and law enforcement with the goal of educating, engaging, and empowering children to recognize potential Internet threats, talk to adults about risks, prevent themselves from being exploited, and report victimization to adults. Separate Websites and resources are available for kids, tweens, and teens.

3. OnGuard Online program (https://www.consumer.ftc.gov/features/feature-0038-onguardonline; Federal Trade Commission) provides instructional material for elementary and middle school teachers, high school teachers, and community educators and resources for parents on how to talk to their children about being online.

During and After an Incident

Students also need to be aware of what to do if they are a victim of an online threat. They can be encouraged to report threats to a teacher, a school counselor, another trusted adult, and the online service provider, if appropriate. Students, teachers, and other members of the public can also contact NCMEC's CyberTipline to report a concern by submitting an online report at https://report.cybertip.org/ or calling 1-800-843-5678.

If somebody is in immediate danger or a crime may have been committed, students, teachers, and staff should contact the school resource officer, police officer, or local law enforcement.

Relation to Emergency Operations Plan (EOP) Development and Planning

The *Guide for Developing High-Quality School Emergency Operations Plans* (*School Guide;* https://rems.ed.gov/docs/REMS_K-12_Guide_508.pdf) was developed in partnership with six Federal departments and agencies, including the U.S. Department of Education, with roles and responsibilities in emergency preparedness. The *School Guide* provides a recommended six-step planning process that is cyclical and ongoing to help schools develop a high-quality EOP and lists several threats and hazards that schools may want to include in the plan, including cyber incidents. This type of threat can be addressed in a Cyber Annex to the EOP, which can address both cyber safety (i.e., the human element) and cybersecurity (i.e., IT systems and networks).

When developing activities to address cyber threats before, during, and after an event occurs, a planning team can progress through the six steps as follows.

Step 1: Form a collaborative planning team. The planning team will likely comprise a core planning team, school personnel, community partners, and a school district representative. To address cyber threats, the planning team can seek the additional input of individuals such as IT staff; local, state, and Federal law enforcement; and emergency management, among others. When identifying actions to address cyber threats to students, the planning team can also look to others who play a role in supporting students' emotional needs, such as a counselor, a bullying coordinator, and other mental/behavioral health professionals.

SIX-STEP PLANNING PROCESS

- **Step 1**: Form a collaborative planning team.
- **Step 2**: Understand the situation.
- **Step 3**: Determine goals and objectives.
- **Step 4**: Plan development (identify courses of action).
- **Step 5**: Plan preparation, review, and approval.
- **Step 6**: Plan implementation and maintenance.

Step 2: Understand the situation. Here, the planning team identifies threats, such as cyber threats, and hazards to the whole school community using a variety of assessment tools, assesses those risks, and prioritizes them for inclusion in the EOP. One assessment that can be especially useful when identifying online threats to the whole school community is a Culture and Climate Assessment. This tool evaluates student, teacher, and staff connectedness to the school and potential behavior problems.

As students can use online platforms, such as social media, to pose or make actual threats to students, teachers, staff, and/or the locality ranging from bullying to targeted violence, another assessment schools should consider implementing is a behavioral threat assessment. The primary purpose of a threat assessment is to prevent targeted violence in schools by students, where a school is deliberately selected as the location for the attack and is not simply a random site of opportunity. More information is available in a REMS TA Center Webinar "Use of Social Media School Behavioral Threat Assessments" at https://rems.ed.gov/TA_Webinars.aspx

Step 3: Determine goals and objectives and **Step 4: Plan development (identify courses of action).** After assessing the level of risk posed by threats and hazards, the planning team should work to determine goals and objectives to achieve the best outcome for before, during, and after an incident. Then courses of action are developed that describe the who, what, when, and how to meet those objectives.

For example, the planning team can address cyberbullying in the EOP by identifying goals and objectives for before, during, and after an incident. The team can then identify courses of action to help prevent incidents from occurring, provide ongoing protection to the student body, mitigate cyberbullying's effects, respond to incidents, and help students recover from an event.

Step 5: Plan preparation, review, and approval. Now a draft EOP is written and circulated to obtain feedback from those responsible for implementing the document. Edits are made based on those comments, and approval is obtained from the appropriate leadership. As the Cyber Annex will address both cyber safety and cybersecurity, this part of the document will include

goals, objectives, and courses of action for keeping both students and the school's IT systems and networks safe.

Step 6: Plan implementation and maintenance. Here, the EOP is maintained via regular reviews and revised when needed. As new cyber threats are constantly emerging, planning teams may decide to review the Cyber Annex more frequently. Further, individuals with roles outlined in the EOP are trained in their responsibilities, and exercises are also conducted to test the school's or school district's ability to respond to a threat or hazard.

Summary

The Internet has brought advantages such as access to information and friends anywhere in the world and at any time. However, it can also serve as a channel to negatively impact students as they unintentionally come across inappropriate content or become the victims of deliberate harassment. To help prevent these incidents from occurring, schools and school districts can create RUPs, filter and block inappropriate content, and promote digital citizenship through instruction on how to stay safe online. If students do become victims, they should be aware of whom they can turn to for help—such as a teacher or other trusted adult. Further, planning teams should consider laying out protocols and courses of action for before, during, and after a cyber incident in the Cyber Annex to the school's EOP as part of their preparedness efforts.

Key Resources

A variety of resources are available to support the cyber safety of students, including:

- Incorporating Sextortion Prevention, Response, and Recovery into School Emergency Operations Plans (EOPs) Webinar, REMS TA Center. This Webinar provided background information on sextortion and discussed how students can be victims and perpetrators. Presenters shared how education agencies can develop measures to prevent and protect students from sextortion with support from local and Federal agencies. http://rems.ed.gov/Sextortion2016Webinar.aspx
- NetSmartz® Workshop Online Program, National Center for Missing and Exploited Children®. This program provides online resources for parents and guardians, educators, law enforcement, teens, tweens, and kids. Information is provided on specific topics, such as cell phones, cyberbullying, and sexting, with accompanying tips and pointers on how to discuss these topics with a child. http://www.netsmartz.org/Parents

- Office of Educational Technology (OET) Web page, U.S. Department of Education. The OET develops national educational technology strategy and policy for how technology can be used by K-12, higher education, and adult education learners. https://tech.ed.gov/
- Privacy Technical Assistance Center, U.S. Department of Education. This Website serves as a comprehensive resource that education agencies can use to get information about privacy, confidentiality, and security practices. The site provides valuable information related to information sharing guidelines, such as the Family Educational Rights and Privacy Act (FERPA), and legislation, such as the Children's Internet Protection Act. http://tech.ed.gov/privacy
- StopBullying.gov Website. This Website (http://www.stopbullying.gov/index.html) serves as a hub of information on the Federal perspective on bullying and contains information and resources to address bullying. Under the Cyberbullying tab, users can access Web pages such as:
  - *Tips for Teachers*, which describes some of the warning signs that a child may be involved in cyberbullying and how to prevent and address cyberbullying; and
  - *Social Media and Gaming*, which lists social media apps and sites commonly used by children and teens and what adults can do to prevent cyberbullying of children who are gaming.

References

[i] "Sextortion: Why Minors Isolate Themselves And Cave Into Perpetrator's Demands," *International Business Times* (http://www.ibtimes.com/sextortion-why-minors-isolate-themselves-cave-perpetrators-demands-2577247)

[ii] "Cyberbullying in city schools soars 351% in just two years," *New York Post* (http://nypost.com/2017/02/01/cyberbullying-in-city-schools-soars-351-in-just-two-years/)

[iii] Effects of Bullying, StopBullying.gov (https://www.stopbullying.gov/at-risk/effects/index.html)

[iv] Children's Internet Protection Act (CIPA), Federal Communications Commission (https://www.fcc.gov/consumers/guides/childrens-internet-protection-act)

[v] "Internet Acceptable Use and Safety Policy (IAUSP)," New York City Department of Education (http://schools.nyc.gov/RulesPolicies/InternetAcceptableUse/default.htm)

[vi] "Inland schools battle online bullying," *The Press-Enterprise* (http://www.pe.com/2017/04/23/inland-schools-battle-online-bullying-social-media-insults/)