FACT SHEET

Sextortion: Protecting Youth Through the School Emergency Operations Plan

READINESS AND EMERGENCY MANAGEMENT FOR SCHOOLS TECHNICAL ASSISTANCE CENTER

Ensuring that students come to school prepared to learn involves comprehensive emergency management planning that supports students in all settings and at all times. This includes protecting students as they participate in online spaces. As Internet communication technology continues to advance, so do opportunities for criminals to entice, exploit, and victimize children online. The prevailing use of mobile devices and the popularization of mobile applications, particularly social media, have given rise to new types of Internet-based crimes, including child pornography, identity theft, illegal access to data, and sextortion.

As the largest group of Internet users and the segment of the population most likely to use social media, youth are among the vulnerable populations at risk of being victimized by cyber-related crimes. To better understand the risks, impacts, and scale of online exploitation of children, the Federal government developed the National Strategy for Child Exploitation Prevention and Interdiction (National Strategy). The National Strategy initiated the National Child Exploitation Threat Assessment, a multiagency effort to analyze and address the risks posed by child exploitation, which includes sextortion as one of five key areas. Using insight gained from a survey of more than 1,000 criminal investigators, law enforcement managers, prosecutors, analysts, victim service providers, and U.S. Department of Justice grant recipients, the Federal government conducted a supplemental assessment. Both assessments identified sextortion as the most significant emergent cyber threat to children and youth.

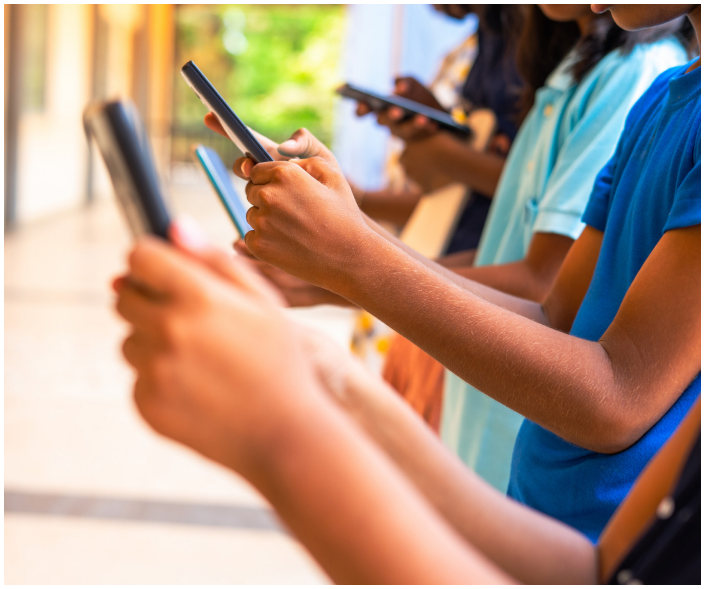
This fact sheet describes sextortion and its impacts on students and outlines how schools can protect youth from sextortion through the creation and modification of a Sextortion Annex in the school emergency operations plan (EOP).

Defining Sextortion

Sextortion is a form of online sexual exploitation and child pornography (when minors are involved) in which offenders use Internet technology to entice, coerce, or blackmail people into sharing sexually explicit images or videos of themselves online. Offenders often manipulate victims into providing sexually explicit images or meeting the offender's monetary or sexual demands by threatening to post the victim's images online or to share the images with the victim's friends and family.

Findings from the National Child Exploitation Threat Assessment revealed concerning trends in the scale and scope of sextortion. Offenders often use a variety of platforms, including social media, chat rooms, gaming platforms, dating apps, and messaging and photo apps, to target, befriend, groom, and coerce hundreds of potential victims. Offenders routinely trick victims by representing themselves online as peers of either the same or the opposite gender. Since 2016, there has been an increase in reported sextortion cases, as well as a shift in whom offenders target and

for what purpose. The National Center for Missing and Exploited Children's (NCMEC) CyberTipline reports that between 2019 and 2021, the number of tips it received involving incidents of sextortion more than doubled. While the dominant motive of offenders previously was to obtain sexual images or favors from victims, increasingly the dominant motive of offenders is to extort money. And, while females aged 10-17 are primary targets, teenage boys are now the most common targets of recent cases.



Although sextortion occurs online and often outside of school hours, it can have resounding negative impacts on many aspects of the victims' life, including their school life. Sextortion victims have reported experiencing depression, anxiety, hopelessness, fear, and other negative mental health impacts; have dropped out of school at higher rates; and have engaged in self-harm, including threatening, attempting, or committing suicide, at higher rates. Because of the immediate and long-lasting, wide-ranging negative effects of sextortion on victims, as well as the frequency with which these crimes occur to students, schools may wish to assess the severity of this threat within their school community. If this assessment indicates that sextortion is a significant threat to the safety, well-being, and continued success of students, emergency planning teams may consider creating and/or enhancing a Sextortion Annex within their EOP.

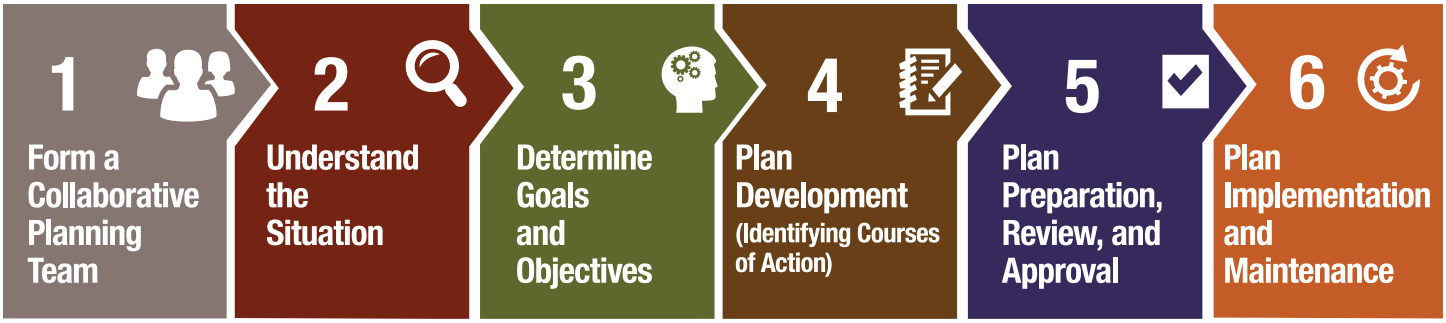
Creating or Enhancing the Sextortion Annex in the EOP

Schools can prevent sextortion within their school community, protect their students from sextortion, mitigate the effects of sextortion, and prepare to respond to and recover from sextortion incidents by developing a Sextortion Annex within their EOP. To support schools, school districts, and other education agencies in planning for and effectively responding to threats such as sextortion, the U.S. Federal government offers several in-depth guidance documents on the development of comprehensive, high-quality EOPs.

The first of these documents, the *Guide for Developing High-Quality School Emergency Operations Plans* (*School Guide*), was released in 2013 and represents a joint effort among six Federal agencies to provide guidance for establishing policies and procedures as well as assistance in creating, reviewing, and maintaining customized and comprehensive school EOPs. In 2019, the *School Guide* was supplemented by complementary guidance, *The Role of Districts in Developing High-Quality School Emergency Operations Plans*. Each document builds upon the National Preparedness System mission areas (prevention, protection, mitigation, response, and recovery) and sets forth a six-step planning process for developing, enhancing, and revising EOPs that address school safety before, during, and after an emergency.

Step 1: Form a Collaborative Planning Team

The six-step planning process offers a framework that ensures that emergency management planning is collaborative and customized to the unique characteristics of the school, district, and situation. Step 1 of this process involves forming a wide-ranging, collaborative planning team of school personnel, community partners, and student/parent representatives to develop a common framework, define and assign roles and responsibilities, and determine a regular schedule of meetings. Membership should include local law enforcement officers, victim service provider representatives, school mental health staff and school psychologists, school-based health professionals, information technology specialists, students, and parents/guardians.



Step 2: Understand the Situation

The *School Guide* emphasizes that effective emergency management planning requires awareness and understanding of the unique circumstances a particular school faces. Once a collaborative planning team is formed, the team can move on to Step 2 to understand the range of threats and hazards and identify the risks posed by sextortion in its school community. Potential data sources for this work include culture and climate assessments and information from local, state, and Federal partners (e.g., the number of reported cases in a school community from law enforcement agencies).

Step 3: Determine Goals and Objectives

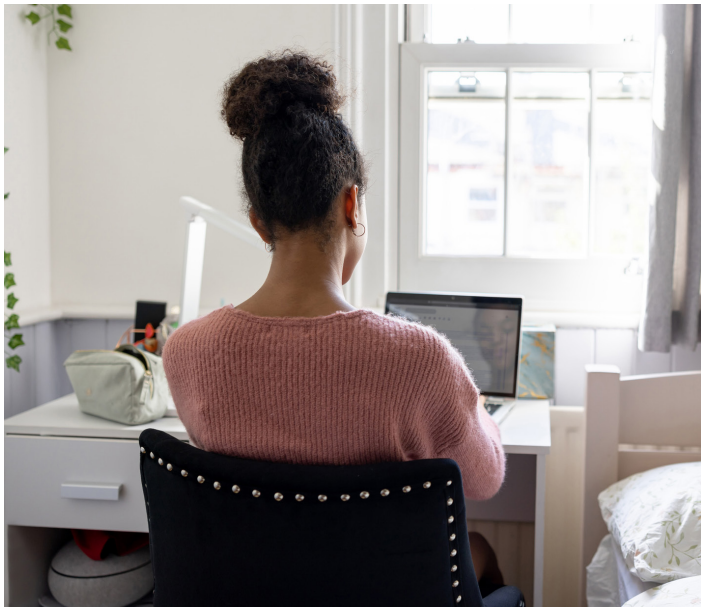
If sextortion is identified as a threat to a school community, planning teams should move forward into Step 3, determining goals and objectives for protecting and supporting students before, during, and after an incident of sextortion occurs. Goals include broad, general statements that describe a desired outcome, while objectives are specific, measurable actions that are necessary to achieve the goals. Sample goals and objectives for a Sextortion Annex are illustrated in the examples below.

- **Goal (Before):** Prevent students from becoming a sextortion victim or predator.
  - **Objective:** Provide sextortion prevention training for all students and staff as a part of health education, cyber safety and cybersecurity, and/or anti-bullying programs.
  - **Objective:** Raise parent and guardian awareness about online safety and sextortion.
- **Goal (During):** Respond to sextortion as soon as an incident is identified.
  - **Objective:** Provide for immediate and short-term medical, physical, and emotional needs of the victim(s).
  - **Objective:** Take immediate protective measures to stop continued sextortion and protect the victim(s).
  - **Objective:** Connect the victim(s) and perpetrator(s) (if applicable) to the appropriate law enforcement and mental health partners.
- **Goal (After):** Restore a safe and healthy learning environment.
  - **Objective:** Provide continued school counseling services to survivors of sextortion.
  - **Objective:** Communicate with stakeholders and the school community.
  - **Objective:** Evaluate and refine plans.

Step 4: Plan Development (Identifying Courses of Action)

Goals and objectives will be the foundation for Step 4, which involves developing courses of action for each identified objective. Courses of action describe the exact tasks that will be completed to meet an objective and include criteria for determining how, when, and by whom each response will be implemented under a variety of circumstances. After completing Step 4, the planning team will have clearly defined goals, objectives, and courses of action to use within the Sextortion Annex. A comprehensive, high-quality Sextortion Annex may include the following courses of action for key populations:

- **School Emergency Managers:** Add sextortion to the list of adversarial and human-caused threats within school EOPs, and work to develop goals, objectives, and courses of action for faculty, staff, and community partners, including law enforcement. Create posters illustrating the legal implications of what happens when a student becomes a perpetrator.
- **School Instructional and Curriculum Development Staff:** Include instructional materials on sextortion as a part of health education, cyber safety and cybersecurity, and anti-bullying programs and/or curricula.
- **School Mental Health Staff:** Evaluate students for risk factors and signs that they are or may become victims or perpetrators of sextortion. Implement counseling services to support sextortion survivors, perpetrators, and families.
- **Teachers:** Review and post checklists on what to do if a student is a victim or perpetrator of sextortion. Refer students to school administration, law enforcement, and social support services if they are a victim or perpetrator of sextortion.
- **Students:** Report incidents of sextortion and suspected perpetrators.
- **Parents/Guardians:** Add layered security to home computers. Teach youth how to identify online enticement and red flags to watch out for. Report incidents of sextortion and suspected perpetrators. Connect victims with immediate, short-term, and long-term support services.



Step 5: Plan Preparation, Review, and Approval

Once goals, objectives, and courses of action are clearly articulated, planning teams can proceed to Step 5 and prepare, review, and share the EOP. During this step, the plan will be formatted, reviewed for compliance with applicable laws, and approved by school leadership and relevant stakeholders. The core planning team should review the Sextortion Annex against policy and guidance put forth from local, state, and Federal agencies. The team may consider comparing it against resources and trainings such as NCMEC's CyberTipline, the Team HOPE program, and digital citizenship and safety program NetSmartz to ensure that courses of action in the Sextortion Annex are evidence based, age appropriate, and aligned with current research.

Step 6: Plan Implementation and Maintenance

Finally, planning teams may proceed to Step 6, implementation and maintenance. This step involves training stakeholders on the EOP; exercising the plan via tabletop exercises, drills, functional exercises, and full-scale exercises; and reviewing, revising, and maintaining the plan after incidents or exercises. Planning teams may find it beneficial to practice the Sextortion Annex by running a sextortion tabletop exercise. Tabletop exercises provide an opportunity for schools to work through a fictional sextortion incident; give core planning teams an occasion to apply courses

of action the school will need to take before, during, and after an incident of sextortion; and offer essential insight into the effectiveness of the Sextortion Annex. The team can then document gaps and strengths in an after-action report and use that information to enhance and maintain the Sextortion Annex.

By using the six-step planning process in the creation of a Sextortion Annex, planning teams can enhance sextortion prevention efforts, reduce response times if a known or suspected incident of sextortion occurs, and implement a comprehensive support plan for student recovery. This planning process also supports the creation and enhancement of EOPs that are informed by national, state, and local research and legislation; framed around prevention, response, and recovery; and designed for sustainability.

Tips to Share With Students

The following section offers tips and information to share with students as they participate in online spaces. School and district administrators, faculty, and staff can use these tips as a part of overall training efforts, as inspiration for checklists and/or posters, and as talking points with students and parents/guardians in conversations about online enticement and sextortion.

Things to Remember

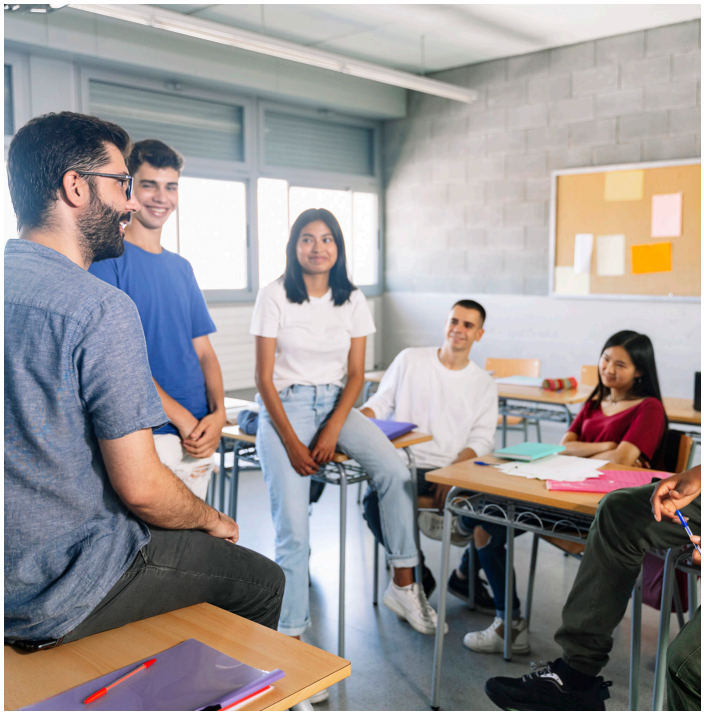
- Anything done online can be seen by and shared with others.
- Video chat sessions can be recorded without one's knowledge.
- Perpetrators can misrepresent themselves online to appear as a fellow student or a caring adult.
- Perpetrators can show a recorded video of a child and make it appear as though it is a live video feed.
- Students should not be afraid to talk to a trusted adult.

Preventing Sextortion Perpetrated by Hackers

- Cover Webcams when not in use to avoid surreptitious recording.
- Use updated antivirus software on all mobile and Internet-connected devices.
- Don't open attachments from anyone you don't personally know.
- Set app and social networking site privacy settings to the strictest level possible.

Risky Behaviors

- Doing anything online that the student does not want shared publicly.
- Sharing explicit photos with anyone online or via text message.
- Engaging in "sexting" — even with a boyfriend, girlfriend, or trusted individual.
- Communicating online or via text with anyone the student does not know personally.
- Befriending strangers on social media, gaming, or other forums/apps/sites.
- Sharing/posting content with strangers (even if it isn't explicit/sexual).
- Sharing or making available personal details/identifiers online.



Related Functional Annexes

While developing a Sextortion Annex, planning teams may identify goals and objectives that fall under the category of an emergency management function. Functions are activities that apply to more than one threat or hazard. Examples of cross-cutting functions that may apply to sextortion threats include the following: public health, medical, and mental health; recovery; and security. Goals, objectives, and courses of action should also be developed for functions, which will eventually become functional annexes in the EOP. Find information on some of the recommended functional annexes that may be activated before, during, and after an incident of sextortion below:

- Public Health, Medical, and Mental Health: How the school will address emergency medical, public health, and mental health counseling issues.
- Recovery: How the school will ensure academics recovery; business services recovery; health, social, emotional, and behavioral recovery; and physical and structural recovery.
- Security: How the school will protect the school community from criminal threats originating from both inside and outside the school.

When referencing the above functions in a Sextortion Annex, the courses of action do not need to be repeated. Instead, add a note that additional information on a particular function may be found in the corresponding functional annex.

Resources

Further Reading — REMS TA Center

- Cyber Safety Considerations for K-12 Schools and School Districts, Fact Sheet
- K-12 Online Classrooms: Emergency Management Planning for All Settings, Fact Sheet
- Addressing Adversarial and Human-Caused Threats That May Impact Students, Staff, and Visitors, Web Page

Training Opportunity — REMS TA Center

- Incorporating Sextortion Prevention, Response, and Recovery Into School Emergency Operations Plans (EOPs), Webinar

Further Reading — Sextortion

- Project Safe Childhood, Website (U.S. Department of Justice)
- Sextortion, Website (U.S. Department of Justice, Federal Bureau of Investigation)
- Violent Crimes Against Children, Web Page (U.S. Department of Justice, Federal Bureau of Investigation)
- Sextortion, Web Page (National Center for Missing and Exploited Children)
- NetSmartz, Web Page (National Center for Missing and Exploited Children)
- Trends Identified in CyberTipline Sextortion Reports, Publication (National Center for Missing and Exploited Children)
- The Online Enticement of Children: An In-Depth Analysis of CyberTipline Reports, Publication (National Center for Missing and Exploited Children)
- Sextortion: Findings From an Online Survey About Threats to Expose Sexual Images, Publication (Crimes Against Children Research Center)
- Sextortion of Minors: Characteristics and Dynamics, Publication (Crimes Against Children Research Center)

READINESS AND EMERGENCY MANAGEMENT FOR SCHOOLS
REMS
TECHNICAL ASSISTANCE CENTER

(855) 781-REMS (7367)

info@remstacenter.org

@remstacenter

https://rems.ed.gov