# Readiness and Emergency Management for Schools (REMS) Technical Assistance (TA) Center

## Cybersecurity and Cyber Safety

Dear School Safety Partner,

Thank you for contacting the U.S. Department of Education, (ED) Office of Safe and Supportive Schools (OSSS) and its Readiness and Emergency Management for Schools (REMS) Technical Assistance (TA) Center with your request for information on cybersecurity for schools and steps education agencies can take, with the collaboration of parents, to protect student privacy while increasing the use of digital learning and video sharing platforms in response to the coronavirus disease 2019 (COVID-19) pandemic.

The onset of COVID-19 has dramatically increased the usage of digital learning formats by education agencies across the nation. As students use the Internet and video platforms such as Zoom and Google Classrooms, they may also become exposed to new threats. Such threats may include data breaches, cyberbullying, inappropriate content, sextortion/ransomware, oversharing, and online predation. Phishing emails, text messages, and scams with COVID-19 themes are also currently trending.

**Report any threats to the National Center for Missing and Exploited Children's CyberTipline by contacting it at https://report.cybertip.org/ or calling 1-800-843-5678.**

Cybersecurity and cyber safety are shared responsibilities of students, parents, and school personnel, especially as more students across the country are learning in the "school at home" setting. This critical topic falls across the school safety continuum (school safety, security, emergency management, and preparedness) and is interconnected with many additional issues. ED's OSSS and its REMS TA Center work in collaboration with and integrate the expertise of our Federal and national partners to address cybersecurity and cyber safety through the

- five National Preparedness System mission areas (protection, prevention, mitigation, response, and recovery);
- comprehensive school emergency operations plan (EOP) development planning principles, especially the need for school safety to address all settings and all times (before, during, and after the school day, in-person and virtual activities);
- broad topic of cybersecurity overall; and
- individual, related threats that schools, students, families, and guardians may face at this time, such as data breaches, sextortion, and human trafficking.

Cyber threats can impact 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.

**Threats Facing School and School District Networks and Systems**
When discussing the topic of protecting student privacy in the school at home setting, it is important to understand the variety of cyber threat types that can weaken school and school district networks and systems, including data breaches, spoofing/phishing, malware/scareware, unpatched or outdated software vulnerabilities, and use of removable media. (Access a list of common threat types.)

Schools and school districts can take a variety of actions to prevent, protect from, mitigate the effects of, respond to, and recover from cyber threats that they may face and that may threaten student privacy. These can be conducted before, during, and after an incident. A sample list of recommendations follows, but note that it is not all-inclusive:

- Work with your IT department to track current cybersecurity trends so that you can provide up-to-date guidelines to educators on the use of video learning platforms.
- Provide cybersecurity and cyber safety education and training to school staff, teachers, students, and families.
- Integrate cyber safety into your EOP's Cyber Annex.
- Use filtering and blocking software to prevent students from accessing inappropriate content and sites that aim to steal their personally identifiable information.
- Create a responsible use policy that outlines expectations for students.
- Incorporate cybersecurity and digital citizenship curriculum into lesson plans.
- Encourage students to report online threats to a teacher, a school counselor, or another trusted adult.

**REMS TA Center Resources**
The REMS TA Center has multiple products that focus on integrating the mission areas before, during, and after an emergency, and that provide information in the context of cyber threats in the school setting, as outlined below:

- Cybersecurity Considerations for K-12 Schools and School Districts. Fact sheet on threats impacting networks and systems and how to prepare before, during, and after an incident. Topics covered include data breaches, denial of service, spoofing/phishing, malware/scareware, unpatched or outdated software vulnerabilities, and removable media.
- Cyber Safety Considerations for K-12 Schools and School Districts. Fact sheet on how schools can address and prepare for online threats to students before, during, and after

an incident. Topics covered include responsible use policies, filtering and blocking content, digital citizenship, education and training, and Cyber Annexes.

- Cyber Security and Protecting Students and Staff Data. Forum on the password-protected Community of Practice for school safety stakeholders to collaborate, share, and learn from the experiences of others in the field.
- Incorporating Sextortion Prevention, Response, and Recovery Into School Emergency Operations Plans (EOPs). Webinar on incorporating sextortion prevention, response, and recovery into school EOPs. It is accompanied by a fact sheet on the same topic and Tips on Protecting Youth From Sextortion.
- Integrating Cybersecurity With Emergency Operations Plans (EOPs) for K-12 Schools | REMS TA Center and U.S. Department of Education. Webinar on the importance of cybersecurity and network protection at K-12 schools.
- Addressing Adversarial- and Human-Caused Threats That May Impact Students, Staff, and Visitors. Web page with more resources on cyber safety, cybersecurity, cyberbullying, sextortion, and other threats.
- Community of Practice (CoP). A secure, online forum is a place for practitioners at schools, school districts, state education agencies, and their community partners to share ideas, experiences, and lessons learned and to engage with one another on the comprehensive topic of preparedness (e.g., prevention).
- Tool Box. An online repository of tools and resources developed by practitioners in the field and pertinent to the needs of school and higher ed practitioners as they engage in school and higher ed emergency management planning.

**National Cybersecurity Resources**

A variety of resources are available from and offered through ED’s Federal and national partners on the topic of cybersecurity, as outlined below:

- National Education Technology Plan (NETP) | OSSS and our colleagues at the Office of Educational Technology collaborated to integrate cybersecurity and cyber safety into the NETP. The Office of Educational Technology plans to expand upon this topic and continues to collaborate with us on a number of activities. For example, through the REMS TA Center, we have worked together to create the resources for K-12 schools shared above.
- Building Technology Infrastructure for Learning | ED’s Office of Educational Technology created this K-12 school infrastructure guide to provide actionable information for school and district leaders. Within this publication is information on encouraging responsible use and digital citizenship.

- STOP.THINK.CONNECT™ | The Cybersecurity and Infrastructure Security Agency leads this national public awareness campaign on taking steps to be safer online and offers student resources and parent and educator resources.
- Project Safe Childhood | The U.S. Department of Justice launched a nationwide initiative to combat child sexual exploitation and abuse.
    - Project Safe Childhood Videos | The U.S. Department of Justice offers videos in English and Spanish on combating child sexual exploitation and abuse.
- Protecting Kids Online | The Federal Trade Commission has a Website for parents on how they can talk to kids about making safe decisions when they socialize online. This includes a Web page, Kids and Socializing Online, and a video, Net Cetera: Chatting with Kids About Being Online.
- CyberTipline | The National Center for Missing and Exploited Children and Office of Juvenile Justice and Delinquency Prevention offer this hotline for reporting any threats.
- NetSmartz® | The National Center for Missing and Exploited Children, with funding from the U.S. Department of Justice, Office of Juvenile Justice and Delinquency Prevention, created this online safety education program with age-appropriate videos and activities.
- Stay Safe Online | The National Cyber Security Alliance offers online safety and digital citizenship resources, such as lesson plans, classroom materials, and discussion guides, to be used at school and at home.
- Be Internet Awesome | Google offers digital citizenship and online safety resources for kids.

We hope that you find the information provided in this response helpful. If you have any additional questions or would like to continue the conversation, please do not hesitate to reply to this message. For additional resources and information on emergency preparedness, please visit the REMS TA Center Website or call us toll-free at 1-855-781-REMS [7367]. We also encourage you to follow us on Twitter.

Thank you, once again, for contacting the REMS TA Center. We appreciate you reaching out to us for assistance!

Sincerely,

OSSS and the REMS TA Center team