Michigan State Police
Office of School Safety

Best Practices for Investigating Student Online Activity

TOOLKIT

Best Practices for Investigating Student Online Activity

School Safety Toolkit Project Funding
This project is supported by Michigan's FY19 STOP School Violence Technology and Threat Assessment Solutions for Safer Schools Program # 2019-YS-BX-0084, awarded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice (DOJ), and administered by the Michigan State Police (MSP). Points of view or opinions contained within this document do not necessarily represent the official position or policies of the DOJ or the MSP.

This resource was developed in partnership with the Michigan School Safety Initiative, which is housed at the University of Michigan Institute for Firearm Injury Prevention.

Michigan School Safety Initiative

INSTITUTE FOR FIREARM INJURY PREVENTION
UNIVERSITY OF MICHIGAN

Published October 2025

1. Introduction

In today's increasingly digital world, the challenges facing educators and school personnel are evolving alongside the rapid growth of online platforms. As students engage more frequently in digital spaces, the potential for harmful or concerning behavior grows, introducing new threats to student safety and well-being.

This toolkit provides guidance for school staff on how to responsibly and effectively investigate online behaviors and content. It equips educators with the knowledge to identify warning signs, interpret digital language (including emojis, slang, and coded speech), and apply ethical decision-making while ensuring compliance with privacy laws. The toolkit emphasizes maintaining student trust and fostering a culture of safety through appropriate boundaries, transparency, and collaboration.

By combining practical steps with legal context and real-world examples, this resource aims to help school personnel respond confidently and consistently to emerging digital concerns, contributing to a safer and more supportive school environment.

2. Legal and Ethical Considerations

Investigating online behavior requires balancing respect for student privacy with the obligation to ensure school safety. Legal and ethical awareness is essential to prevent harm, avoid legal liability, and maintain trust within the school community.

2.1 Understanding Privacy Laws and Regulations

There are three relevant federal laws to consider:

- Family Educational Rights and Privacy Act (FERPA): Limits access to student educational records to authorized personnel, while allowing access when certain exceptions are met, such as in response to court orders or for law enforcement investigations. It is important for schools and their staff to align all evidence-gathering activities with FERPA regulations to protect student privacy. This includes not only restricting records access to authorized personnel, but also ensuring that any information shared meets the criteria for these exceptions. Schools should implement clear policies and provide comprehensive training so that all faculty and staff fully understand and can comply with FERPA requirements.

- Children's Online Privacy Protection Act (COPPA): Prohibits certain online services and websites from collecting, using, or disclosing personal data from children under the age of 13 without permission from a legal guardian and requires opt-in permission to allow targeted advertising to these youth. In educational contexts, schools may provide this consent on behalf of parents or guardians, but only for the use of educational technology services that are solely for the benefit of the student and used within the school environment. This authority does not extend to services intended for commercial use or those that collect data for purposes beyond educational functions. Schools should work with a lawyer to review vendor agreements carefully and ensure that any data collection practices remain compliant with both COPPA and district policies.

- Electronic Communications Privacy Act (ECPA): Protects the privacy of electronic communications by regulating the interception and access of wire, oral, and electronic communications and associated data, establishing legal standards for lawful access by law enforcement.

In addition to federal regulations, schools should also be aware of state-specific privacy laws, including the Michigan Internet Privacy Protection Act (MIPPA). This law prohibits employers and educational institutions from requesting or requiring access to personal internet accounts (e.g., social media passwords) of students or employees, with limited exceptions. While MIPPA allows for investigations into certain misconduct or policy violations, it reinforces the importance of respecting personal digital privacy and due process when collecting online information. Including MIPPA in a school's policy framework helps ensure state-level compliance and protects student rights within Michigan's legal context.

To better understand student data privacy laws and how they apply in school settings, work with a lawyer and see the following resources:

- A Parent Guide to the Family Educational Rights and Privacy Act
- What is COPPA?
- Electronic Communications Privacy Act (ECPA)

2.2 Compliance with School Policies

Before initiating an investigation, it is essential to review and understand the school's existing policies and legal obligations. This guide is not a substitute for legal advice, but rather details best practices for reviewing online information for safety purposes.

To begin the investigation, determine the source of the student's online activity. Identify whether the student is using a personal device, a school-issued device, or accessing a school-authorized account through a third-party service (e.g., student use of school email at a computer in a local library). Verifying the access point is essential, as each scenario may involve different legal authorizations, parental permissions, or policy guidance to ensure compliance with applicable laws and school policies.

It is also important to review the district's Acceptable Use Policy (AUP), which outlines the rules that students agreed to when using school devices, networks, or platforms. These policies often specify behavioral expectations, monitoring permissions, and consequences for misuse. Alongside this, investigators should follow any district- or school-level procedures for initiating, documenting, and escalating investigations. These procedures may designate who is authorized to investigate, what forms should be used, and how findings are reported.

Finally, be aware of any requirements to notify parents or guardians if an investigation is initiated, especially if there is potential for disciplinary action or involvement of law enforcement. Ensure that any resulting disciplinary decisions align with the school or district code of conduct and are applied consistently and fairly.

2.3 Ethical Guidelines for Online Investigations

Laws set clear limits, but when investigating online behaviors, incorporating ethical considerations is essential. The following guidelines provide useful guideposts to ensure investigations are lawful, transparent, and respectful of student rights.

1. **Investigate only public content unless consent is given.** This approach ensures compliance with relevant privacy laws, such as the ECPA.
2. **When reviewing publicly available content, adhere to platform terms and privacy laws.** Avoid using deceptive means to access information. This supports ethical practice, protects evidence integrity, and facilitates collaboration with law enforcement when necessary. Capture screenshots with embedded time and date stamps to preserve relevant evidence in a format that supports admissibility and facilitates use by law enforcement.
3. **Establish clear protocols for documentation and information sharing.** Ensure compliance with laws such as FERPA and ECPA by creating investigation records that are securely stored and accessible only to authorized personnel.
4. **Use standardized forms or digital logs to document evidence collection.** Record the time, date, and method of information collection to develop a clear chain of custody and ensure evidence integrity.
5. **Collaborate with law enforcement to ensure evidence meets legal standards, if necessary.** Notify law enforcement when credible online threats are discovered to ensure evidence collection complies with legal standards.
6. **Employ reliable digital forensic tools to capture and store data without alteration.** Preserve digital evidence in its original form to protect integrity, consistency, and legal defensibility. Tools such as FTK Imager can help document and safeguard investigative findings. Evaluate these tools regularly to keep them up to date and provide training for staff in their use.

The resources below offer practical guidance on selecting, using, and maintaining digital forensic tools to ensure proper evidence handling in school investigations:

- A guide to digital forensics data acquisition with FTK Imager
- U.S. Department of Homeland Security - Digital Forensic Tools

3. Recognizing Concerning Behavior

Recognizing signs of distress, risk, or concerning behavior in students' online activity is an essential part of ensuring student safety and supporting early intervention. This section outlines examples of content that may warrant attention, along with guidance on why certain warning signs matter in a school setting.

3.1 Overview of Behavioral Indicators

While every student's digital footprint is different, certain patterns and types of content may raise red flags for educators, counselors, or administrators. Recognizing these indicators can help ensure that students receive timely support.

Violent or Threatening Content
Posts that reference violence, whether toward others or oneself, should never be ignored. Even if these statements appear to be jokes or expressions of frustration, they may indicate deeper emotional struggles or, in some cases, genuine threats.

Signs of Emotional Distress
Expressions of hopelessness, self-harm, or suicidal ideation often appear online before a student reaches out in person. These may take the form of captions, coded language, or shared images that hint at emotional distress.

Online Bullying and Harassment
Online bullying and harassment are also common forms of concerning content. These behaviors can include repeated insults, exclusionary behavior, hate speech, or sharing harmful memes. Students on the receiving end of such behavior may experience emotional harm, while those engaging in it need clear guidance to recognize and take responsibility for their actions.

Grooming and Exploitation
Some students may also be vulnerable to online grooming or exploitation. Communications that seem secretive, overly personal, or sexual in nature, especially with individuals outside the student's peer group, may indicate attempts at manipulation or abuse. Educators should also be alert to signs of students sharing explicit images, disclosing too much personal information, or engaging with individuals who appear to be seeking control or influence.

Other Concerning Behaviors
Other warning signs include references to substance use, illegal activity, or sudden shifts in how a student behaves online, such as withdrawing from friends or posting dark or extreme content. In some cases, students may begin engaging with radicalized or extremist ideologies, which can start subtly and escalate over time.

It's important to keep in mind that context matters. One concerning post may not, on its own, warrant alarm, but consistent patterns, sudden changes, or clear expressions of harm to self or others should always prompt action. Document what is observed, avoid assumptions, and follow school protocol to determine the appropriate next steps.

By staying attentive to these indicators and responding thoughtfully, school personnel can help ensure that students receive support before issues escalate into crises.

3.2 Concerning Content and Behavioral Indicators

The sections below provide examples of specific content that may require further investigation. Consider the content in the context of the student's behavior. If the context is unclear or escalating behavior is noticed, follow the school's reporting protocol and consult with the school's Behavioral Threat Assessment and Management (BTAM) team.

Please note that escalating behavior might include increasingly aggressive or threatening language, sudden changes in behavior, expressions of intent to harm oneself or others, fixation on violent events or individuals, withdrawal from usual activities, or an accumulation of concerning incidents over time.

Firearms, knives, and other weapons

What to look for:
- Mentions, images, or videos of guns, knives, or explosives.
- Posts showing handling, modifying, or glorifying weapons.
- Searches for videos using weapons.

Why it matters:
- May indicate the threat of violence or fascination with weapons.

Additional notes:
- Evaluate the content to exclude concerns about legal/hobbyist use (e.g., hunting, Olympic sports).

Violent language

What to look for:

- Hostile or threatening words.
- Glorifying harm or revenge.
- Direct or coded threats.

Why it matters:

- May suggest intent to harm others or preoccupation with violence.
- May indicate support for someone else in the school community acting this way.

Hate language / ideology

What to look for:

- Racist, misogynistic, anti-LGBTQ+, xenophobic, or extremist content.
- Incel or white supremacist references.
- Language that degrades, blames, or dehumanizes particular groups.
- Slurs, coded phrases, or hashtags associated with extremist rhetoric.
- Celebration or justification of violence based on identity.
- References to ideologies rooted in gender supremacy, racism, or homophobia.

Why it matters:

- May indicate exposure to radicalizing or harmful beliefs; can promote group-based violence.

Additional notes:

- **Resource:** For a glossary and a list of latest terms, visit Center for Extremism - Glossary of Extremism and Hate.

Idolization of prior attacks

What to look for:

- Posts admiring mass shooters.
- Countdowns to anniversaries.
- Use of known shooter names.

Why it matters:

- Indicates identification with past perpetrators and often precedes threatening behavior.

Alcohol / drugs

What to look for:

- References to pills, marijuana, alcohol, vaping, or other substances; images or slang suggesting use.

Why it matters:

- May signal substance use or access, especially when paired with other risk indicators.

Sexting / sensitive images

What to look for:

- Nude or suggestive images, especially involving minors.
- References to sharing explicit content.

Why it matters:

- Possession or distribution may violate child sexual abuse material laws and carry serious legal consequences.
- **Resource:** Michigan Law on Child Sexually Abusive Material (MCL 750.145c)

Additional notes:

- Do not save or redistribute the image.
- Follow school reporting procedures immediately.
- Understand that even possession may trigger mandatory reporting laws.
- Educate students and parents proactively about these risks and school policies.
- Be aware that students may be coerced into providing sensitive materials, and address these situations with appropriate support and intervention strategies.
- **Resource:** Take It Down

Money

What to look for:

- Images of large amounts of money, “flexing,” or cash handoffs.

Why it matters:

- Could indicate involvement in drug sales, theft, or online scams.

Threatening behavior

What to look for:

- Direct threats (“I’m going to…”).
- Vague ominous statements (“Watch what happens tomorrow”).

Why it matters:

- Can be early indicators of planned violence or retaliation.

Bullying / cyberbullying

What to look for:

- Repeated harassment.
- Targeting individuals.
- Exclusionary group chats.
- Degrading messages.
- Social media posts.

Why it matters:

- Increases the risk for emotional distress and may provoke retaliation or self-harm.
- It often targets vulnerable students.

Artificial intelligence (AI) content

What to look for:

- Deepfakes.
- Synthetic pornographic images.
- Voice simulations.
- Altered videos.

Why it matters:

- May be used for bullying, blackmail, or misinformation
- Creation or distribution may be illegal, especially involving minors.

Trending Emojis

What to look for:

- Use of symbols like 🔫 (gun), 💊 (pill), 🍑/🍆/💦 (sexual).

Why it matters:

- Emojis may be used to hide meaning from adults or systems.

Additional notes:

- Understanding context is critical.
- See **Appendix B: Emoji Interpretations & Flags for Concern**.

Trending hashtags

What to look for:

- Hashtags are often used in extremist or harmful online communities.

Why it matters:

- Used to categorize and organize content across social platforms, and to connect with like-minded individuals.

Additional notes:

- Monitoring trending hashtags helps track risky topics and potential threats.
- Be mindful that hashtag meanings may be coded.
- Some coded hashtags include: #anas (anorexics) #mias (bulimics) #sue (suicide), #cuts (self-harm), #kush and #420 (marijuana).
- **Resource:** SmartSocial.com regularly updates a list of teen slang, social media terms, popular acronyms, secret emoji meanings, and dangerous hashtags.

4. Investigating Student Online Behavior

4.1 Principles and Best Practices for Investigating Online Behavior

- **Build trust with students and maintain open communication.**
  Establish a trusting relationship with students to encourage open and honest dialogue. Engage with students regularly and practice active listening. When students share concerning information, ask open-ended questions to gather details. Remember that online behavior may indicate that the student is a victim or is being manipulated by other students or adults with criminal intent.

- **Utilize external resources for current guidance.**
  Stay informed about digital literacy, safety, and investigative best practices by regularly consulting reputable resources. Doing so will help recognize emerging digital threats and strengthen approaches to online investigations.

Recommended Resources for Digital Literacy and Safety

- Common Sense Media: Offers resources on media literacy, privacy, and digital citizenship.
- The Family Online Safety Institute (FOSI): Provides guidance to help parents and students improve their knowledge of digital safety.
- See **Appendix A** for additional resources.

- **Promote collaboration and effective reporting.**
  Collaboration and timely reporting help address concerns comprehensively and reduce future risks. Work closely with administrators, counselors, and school resource officers to ensure that all concerns are thoroughly investigated and that plans are in place to address both current and future issues. Share relevant information through established reporting channels to support timely interventions. If the person reporting cannot reach someone right away or prefers to report confidentially, consider using Michigan's designated confidential reporting system, OK2SAY. Always follow the school's established protocols for BTAM.

OK2SAY is Michigan's confidential tip line for students and community members to report threats, bullying, or concerning behavior. Tips may be submitted 24/7 and are routed to the appropriate school officials or law enforcement for a timely response.

4.2 Following School Protocol - Who to Contact and When

Adhering to school and district protocols is critical when investigating and addressing concerning online content. Each school should have established procedures for documentation, escalation, and communication. Acting consistently and appropriately ensures student safety and legal compliance.

Report Concerns When:

- Observing content suggesting current or future plans for self-harm, harm to others, or any credible threat.
- A student discloses concerning digital activity, whether about themselves or someone else.
- Discovering explicit images or videos shared by or involving minors.
- Observing cyberbullying, hate speech, or targeted harassment.

Who to Contact:

- A designated school administrator or principal.
- A member of the school's Behavioral Threat Assessment and Management (BTAM) team.
- School counselors or mental health professionals.
- School resource officers or local law enforcement, especially when there is an immediate or credible threat or illegal content.
- OK2SAY, Michigan's confidential reporting system, to safely report misconduct or safety concerns, especially in sensitive situations.

Always document concerns and share them proactively with the appropriate personnel in accordance with laws, school policies, and guidelines. If there is uncertainty about the correct process, seek guidance from the school's administrator to ensure the proper steps are followed.

4.3 Tools and Techniques for Online Investigation

Effectively investigating online content requires familiarity with a range of digital tools and platforms. This section details resources school personnel can use to identify, verify, and analyze online behaviors, along with key considerations for conducting thorough and responsible investigations.

Tool / Technique	Use Case	Key Considerations
Google Reverse Image Search TinEye	Identify where an image first appeared to assess its credibility. Determine whether an image has been reused, manipulated, or taken out of context.	Examine image metadata*; be aware that reverse image search results may require careful, manual interpretation. *Metadata refers to hidden information embedded in an image file, such as the date, time, location (GPS), and device used to capture the image.
Emojipedia	Provides up-to-date definitions and meanings of emojis.	Keep in mind that meanings can evolve quickly; always consider context and cultural variations.
Urban Dictionary	Helps decode student slang and internet terminology.	Definitions are user-submitted; always cross-reference with reputable sources such as standard dictionaries, news articles, or academic references to avoid misinterpretation.
School-Issued Device Monitoring	Review browsing history, messaging apps, shared documents, and login patterns on school-issued devices.	Always follow school policies on digital privacy and access; document findings carefully.
Google Alerts	Receive email notifications for specific topics, trends, or keywords, such as “new teen app” or “school threat.”	**Resource:** How to Set Up Google Alerts

Tool / Technique	Use Case	Key Considerations
Social Media Platforms	Where to look for information: ● Website history (e.g., YouTube, Reddit). ● Telegram. ● Discord. ● 4Chan, Pol, Board. ● TikTok. ● Instagram. ● Snapchat.	Some platforms are encrypted or have temporary content (e.g., Snapchat); capture screenshots immediately if needed. **Resource:** Safer Schools Together's Raising Digitally Responsible Youth resource provides an overview of popular social media and gaming platforms.
Boolean Operators	Filter search results in Google, shared drives, or inboxes more precisely using AND, OR, NOT logic.	Requires logical syntax; improperly structured searches may miss relevant information. **Resource:** AND, OR, NOT - Which to Choose? Boolean searches explained
AI Detection Tools	Identify, evaluate, or flag synthetic media, including deepfakes, manipulated images, and fake audio. Such content may be used in bullying, impersonation, blackmail, or simulating harmful content.	Tools like FotoForensics and Deepware Scanner can help analyze images for signs of manipulation or AI generation. Be aware that AI filters may mask activity to evade detection. Key indicators to look for: **Visual:** Unnatural textures, pixelation, warped symmetry. **Audio:** Inconsistent speech cadence, robotic tone.

Appendix A: Resources for Digital Literacy and Safety

Parent Guides (ConnectSafely.org): Printable guides covering topics such as privacy, cyberbullying, and specific apps, like Snapchat and Instagram.

Media Smarts: Provides resources on cyberbullying, privacy, and misinformation.

Cyberwise: Focuses on education about social media, privacy, and internet security.

National Association for Media Literacy Education (NAMLE): Provides resources for media literacy education.

Get Safe Online: Offers practical advice on cybersecurity and privacy.

Appendix B: Emoji Interpretations and Potential Concerns

Emoji	Possible Meaning(s)	Contextual Notes
🔫 (water pistol)	Gun / threat / violence	May suggest aggression or intent to harm; always consider tone and accompanying content.
💊 (pill)	Drugs / misuse of medication	Common in discussions about Xanax, opioids, or prescription abuse.
🥃 / 🍷 / 🍺 (glass / mug)	Alcohol	May appear in posts about underage drinking or partying.
🌿 / 🍁 / 🚬 / 🥦 (leaf, cigarette, broccoli)	Marijuana / smoking	Often associated with cannabis use; may also include references to “420.”
💵 / 🤑 / 💰 (money)	Money / “flexing” (bragging)	Can indicate wealth, a desire for money, or involvement in financial transactions, sometimes linked to risky or unethical behavior.
🔥 (fire)	Hype / "lit" / destruction	Often signifies excitement, but can also appear in threats of arson or destruction.
😈 / 👿 (smiling / angry face with horns)	Mischief / harmful intent	May suggest intent to harm, especially when paired with violent captions.

Emoji	Possible Meaning(s)	Contextual Notes
🍑 / 🍆 (peach, eggplant)	Sexual imagery (body parts)	Common in sexting or explicit messages.
💦 (water droplets)	Ejaculation / arousal	Often combined with 🍑 (peach) or 🍆 (eggplant) in sexual contexts.
📸 / 👻 / 🔥 (camera, ghost, fire)	Snapchat references	May indicate sexting, temporary messages, or message streaks.
🐀 (rat)	Snitch / betrayal	Often used to imply betrayal or "snitching," especially in contexts involving broken trust, secrets, or perceived disloyalty.

Note: Emoji meanings evolve over time and depend heavily on context, combinations, and cultural use. When in doubt, examine posts holistically or use tools like Emojipedia for updated interpretations.

Safer Schools Together's International Center for Digital Threat Assessment offers guidance on Interpreting and Translating Emojis.

SmartSocial.com regularly updates a comprehensive list of teen slang, social media terms, popular acronyms, secret emoji meanings, and dangerous hashtags.