If the incident involves criminal activity;

STOP!

Do not take any further action until you have consulted with law enforcement officials.

LEARNING MODULE A

Prepare for an Incident

Some digital incidents will require significant preparation to ensure positive outcomes for all parties involved. This learning module will identify the necessary preparations that will help administrators feel confident and prepared as they manage an incident.

BUILD RELATIONSHIPS WITH LAW ENFORCEMENT AND KEY PERSONNEL

Where an incident violates state law, an investigation is complicated by the myriad of legal issues involved, including privacy, freedom of speech, and search and seizure laws. As an employee of a public school, you are considered an agent of the state and therefore subject to applicable search and seizure and privacy laws and must follow the lead of law enforcement for how evidence must be handled. Private school employees do not have the same level of obligation, as they are not agents of the state but should still make every effort to conduct "reasonable" investigations.

An important first step is to create a strong working relationship with local law enforcement, the district attorney's office, legal counsel for the school, administrators, teachers, school resource officers and school psychologists. A committee comprised of these individuals should be formed to establish relationships, encourage communication and to ascertain expectations before an incident occurs.[1]

The tools and professional development will help schools navigate this process, giving guidelines that comply with federal law, but it should not be construed as specific legal advice. Schools and districts should seek out state and school leaders to affirm that school policies are in line with state laws and timeline requirements for reporting.

Given the potential criminal issues involved in some cyber incidents (e.g., sexting, some harassment, incitement), it is imperative that school districts develop a clear protocol for responding, reporting and investigating incidents that violate state law. This protocol must be developed in cooperation with the local district attorney and school district counsel. It should also address the standards for search and seizure, when to contact law enforcement, and the handling of cell phones and other digital devices that could contain illegal data, such as child pornography.

The committee should review parameters for how and when incidents should be reported to authorities and investigated. For example, law enforcement may provide schools with guidance on whether they wish to be involved in pure sexting incidents (photographs consensually created between minors) that have not been spread beyond the two involved and was a "first offense." In addition, clear direction about how to handle digital evidence would be mutually beneficial to law enforcement and administrators to ensure that evidence is properly maintained and to give administrators the necessary knowledge so that they do not inadvertently expose themselves to criminal prosecution.

In addition, the committee should develop protocol to ensure all school personnel know to whom they should report and how images and cell phones should be handled.

Establishing guidelines for how to handle incidents before they occur not only will help a school be ready when an incident arises, but it will also allow schools to communicate with parents and students and give them notification about how illegal incidents (such as sexting) will be handled.

PREPARE A SECURE REPOSITORY FOR EVIDENCE STORAGE

Schools should prepare procedures and a location for data and evidence storage that is reliable and secure in the event of an incident. Designate an external hard drive that can be easily locked in a secure cabinet or desk for the preservation of digital evidence.

1. **Initiate a Preservation (Litigation) Hold**
    a. The law requires that once a school reasonably anticipates litigation, it is obligated to suspend its routine document retention/destruction policy to ensure the preservation of relevant documents. Though not every complaint or instance of misuse of technology will necessarily lead to litigation, consider whether the circumstances and/or the severity of the allegations warrant a preservation hold.
    b. Notify employees who might come into possession relevant documents and data of the obligation to preserve what they have. The following information will help define to scope of the preservation hold.
        i. Who are the custodians? This likely includes the employees responsible for site-level and district-level network administration, but extends to any employee likely to have relevant information.
        i. What are the relevant dates or date ranges?
        ii. What is the key subject matter?
        iii. Where is the data stored? (e.g., is it stored on local computer or laptop hard drives, on networks maintained at the site- or district-level, or outside the district's system by third parties, such as internet service providers?
        iv. What types of documents and data should be stored? Electronic documents include email messages and attachments, word processing documents, graphic images, and spreadsheets. The data stored also includes "metadata," the hidden or embedded electronic information about a document, such as its author, when it was created, when and how it was modified, when an item was received and opened or accessed, and whether it was copied to anyone.
2. **Physically Preserve Evidence**
    a. Act quickly: Electronically stored information can be lost or destroyed very quickly, making further investigation more difficult and costly, if not impossible.
    b. Check Everywhere: As staff and students become increasingly more "tech-savvy," the need to think creatively for all possible sources of data becomes even more important. Information technology staff and/or computer forensic specialists can help identify sources of electronically stored information and how they are or might be connected, such as the following:
        - Hard drives of desktop computers, laptops, netbooks, and tablets/slates
        - Network servers (site- and/or district-level servers)
        - Portable media (CDs, DVDs, flash drives, memory sticks, portable hard drives)
        - Mobile phones/PDAs/Smartphones: Cell phones have the capacity for storing immense amounts of private information. Unlike pagers or address books, modern cell phones can record incoming and outgoing calls, but also contain address books, calendars, voice and text messages, email, video and pictures; and are capable of storing highly personal information, such as the user's most private thoughts and conversations.
        - Backup tapes and email archives
        - Printers: If printers can be accessed quickly enough after an alleged technology-related incident, documents may still be in the "buffer."
        - Logs and data available through firewall programs and spam filtering software
        - External websites

3. **Confiscate and store equipment and media in a secure location**

    iv. Depending on the source of electronically stored information, different preservation techniques may be in appropriate to prevent documents from being destroyed or hidden data from being changed. A faraday bag can be used to store portable media (such as cell phones) to help ensure that they are not accessed remotely.

    v. Computers should be removed (i.e., disconnected immediately from power sources, ethernet connections, and phone lines) and secured. If the hardware is still needed for employees to perform their duties, remove the hard drive(s) for storage and replace with a new hard drive.

    vi. Portable media should be taken into custody and secured.

    vii. The physical back up tapes, disks, and the like, should be preserved to avoid inadvertent re-writing of data during future backups and archive activities.

    viii. Maintain chain of custody logs and procedures (such as use of sealed evidence bags), so it can later be proven who had access to the media and when.

a. Prevent unauthorized access: Preserving electronically stored information will also require proactive steps to prevent certain faculty/staff from accessing data, such as blocking of user ID numbers and remote access capability.

b. Maintain hard copy documents already generated (to the extent they already exist and may lawfully be retained).