IRT Overview

This free resource, the ICAC/iKeepSafe Incident Response Tool for Schools (IRT) helps with the steps of incident management, such as fact-finding, documentation, reporting and engaging the appropriate school officials and other stakeholders. Through the use of this tool, ICAC's and all law enforcement can help schools plan and prepare an effective and appropriate response to all types of technology related incidents, including cyberbullying, sexting, hacking and threats of violence that involves students and/or staff.

Often, school personnel are the first to identify an issue involving a student(s) and this tool provides guidelines and direction for an effective response. The IRT will promote communication with schools and establish a proper investigative response that, when necessary, preserves evidence and protects victims.

The general hope with the IRT is that it will be used to assist both schools and law enforcement with establishing a plan of action for the response to the variety of technology related incidents that take place frequently in schools. By using this tool, a discussion between schools and law enforcement can limit inappropriate responses and establish an effective and collaborative victim-centered response.

Of note, the flowchart and numerous documents have a disclaimer; "If the incident involves criminal activity; STOP! Do not take further action until you have consulted with law enforcement officials". It is important to have conversations and makes plans between law enforcement and schools regarding how all types of incidents should be handled. This includes what constitutes a crime, who will contacted and steps to preserve evidence. Training should include how the IRT Flowchart can assist in the management of an incident and who is responsible for each stop of the investigative process.

Each of the following are downloadable for printing.

IRT Flowchart: This is a flowchart that directs the workflow for a response to a technology related incident. It starts with the report of an incident and guides the evidence collection, the investigative process, the need to include others and follow up and support. It is recommended that a printed copy is posted in school offices for immediate reference when needed.

IRT Flowchart with Instructions: This 14 page document provides detail information regarding the use of the IRT Flowchart. This includes documentation, evidence collection and storage, investigative process, whom to contact, response steps and incident evaluation.

IRT Investigative Report Form: This 20 page form is similar to a police report form and helps schools create a record of the incident. This includes General Incident Information, Law Enforcement Contact, Victim information, Offender Information, Witness Information, and Staff Contact Information.

IRT Supplemental Report Form: This 3 page form provides relevant questions and information to be documented as a supplement to the original report form.

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 and others feel confident and prepared as they manage an incident.

Learning Module B – Conducting an Investigation: You may be dealing with allegations that staff, students, or others have used technology to hack the network, view pornography, engage in harassment, cheat, or otherwise inappropriately use technology. Regardless the situation, one of the most critical aspects of responding is the ability to conduct an effective investigation without violating free speech, privacy, search and seizure laws, and without destroying evidence.

Learning Module C – Conducting an Interview: This Learning Module addresses the gathering of evidence both through interviews and through electronically stored information. You will need to determine, given the facts and circumstances of the particular case, the appropriate sequence of interviews in relation to collecting other evidence.

Learning Module D – Search of a Cell Phone: Depending on the laws in your state, you likely have limits on when and why you can look into a student's cell phone. Your school or district/regional Responsible Use Policy (RUP/AUP) will also affect how much authority you have to confiscate a phone if it causes a disruption in class, is used for cheating, or if you reasonably suspect the phone contains harmful or illegal materials.

Learning Module E – Acceptable Use Policy: Whether the documents governing technology at your school site are referred to as "Acceptable Use," "Responsible Use," or simply "Technology Use" policies, it is likely time to rethink or update such documents. In doing so, each educational institution must acknowledge that technology use policies are not single, "one-size fits all" documents and need which can be adopted nationwide and on a one-time basis.

Learning Module F – Data Privacy: Education technology and cloud-based services offer important new opportunities and efficiencies for schools. In order to reap the benefits of education technology, the whole school community (educators, school staff, administrators, district leadership, parents and students) need transparency and understanding about student data: what is collected, how it is used, who else may have access to it and the protections in place for its storage and disposal.