Flowchart Instructions

If the incident involves criminal activity; STOP, do not take any further action until you have consulted with law enforcement officials.

School administration receives notice of a technology-related incident

You should automatically treat any technology-related incident that occurs **on school property** as an incident of concern. Technology-related incidents that occur off-campus can also be categorized as incidents of concern if they:

- Create substantial disruptions at school
- Interfere with a student's right to learn in a secure environment
- Pose a threat to a student or staff member

Preserve evidence (physical and digital)

This crucial step should be treated with as much care as possible to protect the feelings of all parties involved. The process of preserving evidence will inevitably cause stress and anxiety for some people. After you collect and preserve any relevant evidence, your e-safety coordinator should immediately attend to the emotional needs of the people involved.

Before you begin an investigation in earnest, your principal or e-safety coordinator should take immediate care to preserve any evidence that has materialized in the course of discovering the incident. You should exercise extreme care when preserving evidence to avoid:

- Attempts by offenders and others to tamper with or delete evidence.
- Contamination of evidence
- Possession of illegal or incriminating data on school or employee devices

Involve ICT/Technical staff (as needed)

If a technology-related incident occurs on a school network or computer, call in your technical/ICT staff to capture the evidence. This includes:

- Printing physical evidence in the form of screen shots (website pages, file folder structures, etc.).
- Identifying computer systems that were used, securing the scene, and preserving trace evidence.

- Collecting all relevant digital evidence, including document screens, system time, and network activity.
- Noting any plainly visible cyber trails.
- Preserving the contents of RAM memory if needed using approved tools and procedures.
- Properly securing complete computer systems when necessary, including photographing, labeling, and documenting system details on the appropriate collection form. You should also disconnect network, modem, and power cables; collect relevant software and peripherals, and secure related documentation, removable media, passwords, etc.

Evidence storage

You should prepare a plan for evidence storage *before* an incident occurs. This includes:

- Preparing a secure Preservation Hold that will ensure that evidence will not be contaminated or altered.
- Maintaining a chain of evidence log that records everyone who has access to the evidence, including staff members with keys to storage cabinets and desks.

Examples:

Storage Scenario 1: A mobile phone is seized by a teacher. The screen shows illegal or unlawful behavior. *Without searching through or looking at* the contents of the mobile phone, seal the phone in an evidence bag (or ziplock bag) and secure it in the Preservation Hold until the preliminary investigation occurs.

Storage Scenario 2: An RUP/AUP violation occurs on a school computer. The ICT/Technical staff removes the computer to a secure cabinet until that data can be backed up to a secure external hard drive.

Additional Resources:

Learning Module A: Prepare for an Incident Learning Module D: How to Conduct a Reasonable Search of a Cell Phone

Provide support for students and other parties

In addition to launching an investigation and properly securing evidence, you should carefully consider the needs of all the affected parties. This includes attending to the rights and dignity of all parties involved. Whenever possible, offer counseling services and work to re-establish a safe environment in your school.

Conduct a preliminary investigation (using investigation forms)

After you attend to the affected students and properly preserve the evidence, begin a thorough preliminary investigation of the incident. For detailed information on how to conduct a proper investigation, review Learning Module B: How to Conduct an Investigation.

Investigation forms

iKeepSafe has developed a collection of tools and resources to help you conduct proper investigations, including an interactive online Incident Response Tool and a collection of Incident Response Forms. As you begin your investigation:

- Review the information in Learning Module B: How to Conduct an Investigation.

- Use the online Incident Response Tool to generate customized recommendations and next steps based on how you answer specific questions about the incident you're dealing with.

Take advantage of a set of 7 generic Investigation Forms that will guide your efforts to properly investigate incidents. You can print these forms or save them to a dedicated folder on your desktop.

Do you suspect illegal, unlawful, or harmful activities?

You should report any communication that may cause serious harm or reveal illegal or unlawful activities to local law enforcement immediately.

In most cases, you should also notify district administrators and consider bringing in legal counsel.

These inappropriate employee communications may include content that violates a range of different laws, including:

- Discrimination
- Retaliation
- Harassment
- Defamation
- Network hacking
- Viewing and/or transmitting pornography.

If illegal behavior by a student or staff member is suspected, you have a duty to consult with the police at the earliest opportunity, preserve any potential evidence for school records, and hand that evidence over to the police. You may also need to report the incident to other outside agency.

Child Pornography Warning

Discovery of child pornography or having a reasonable suspicion of child pornography on school equipment or the school's network is a very serious situation, which should be reported to the police immediately.

Do not download, print, or otherwise preserve any data containing child pornography, as this may implicate you or other school employees in the crime.

If you discover or suspect child pornography on a school computer, leave the device exactly as it is (turn off the screen if child porn is on screen), and call police immediately. Make notes regarding your suspicions, what you saw yourself, and what was reported to you. Date your notes and preserve them in a secure location. Do not let anyone near the equipment, and record the event in the school Incident Log. If no log exists, begin one with this incident.

Contact district administration for access to legal team

If you suspect serious harm or illegal/unlawful activity, call your district or regional lawyer at the same time you contact law enforcement.

If you believe the incident could be made public through the media, cause a disruption in the school, or result in possible harassment or discrimination litigation, you should contact district-level administration and request legal counsel. Your district's administration and legal department will also be able to provide the best support and guidance for managing these types of legal or PR problems.

In many school districts, only district administrators are authorized to contact legal counsel, so check your district's guidelines and follow the appropriate procedures.

Call law enforcement or child welfare agencies

Any communication that shows the potential for serious harm or illegal/unlawful activity should be reported to local law enforcement immediately. This includes:

- Evidence that someone on or off campus is in danger of serious harm (e.g. plans for a gang fight, plans to hurt someone, etc.)
- Evidence of intent to commit suicide
- Evidence of sexually explicit photos of a minor (e.g. pictures of another student)
- Inappropriate contact between a student and faculty or staff member (adult and minor)

If you find evidence of child pornography or have a "reasonable suspicion" of child pornography, call the police immediately. Law enforcement officials may need to collect evidence, so work closely with them to coordinate next steps. **Do not** copy, preserve, or otherwise store digital data that might contain child pornography.

Retain as much of the evidence as the law will allow to support your own internal investigation, because after you surrender evidence to law enforcement you may not be able to access it again.

Your school is required to continue its investigation and document evidence even after the police take over the investigation. A collaborative working relationship with law enforcement where both parties are willing and motivated to openly share information will produce the best results for both the school and the police. Sharing information will enable your school to proceed with a disciplinary hearing independent of any criminal case.

If you suspect a student is being abused by anyone, you should also contact the appropriate child welfare agency at the same time you reach out to law enforcement.

Most states have mandatory reporting guidelines for reporting child abuse or neglect. A reasonable suspicion of abuse legally obligates you to contact child welfare agencies. In these cases, you do not have the burden of proof. You must only demonstrate a "reasonable suspicion" that abuse has taken place.

Release evidence to agencies

Any evidence you preserve should be shared with law enforcement or any other agency that assumes jurisdiction over the investigation.

Retain as much of the evidence as the law will allow to support your own internal investigation, because after you surrender evidence to law enforcement you may not be able to access it again.

Could this incident create legal or PR problems for the school?

Legal and PR problems (potential litigation, negative media attention, or a strong community reaction against the school) can create serious issues for your district—even in situations that don't involve law enforcement.

In these types of Tier 2 situations, you should notify the school or district attorney and district administration immediately.

Do you still consider this a serious incident?

Many Tier 2 technology-related incidents require serious attention—even when they don't involve illegal activities or create legal or PR problems for your school. These can include:

- Incidents that involve repeat offenders or students at risk for future crimes
- Plagiarism and cheating

Other technology-related problems that your school is working to eliminate, particularly when they involve repeat offenders

Determine how to engage parent(s)

Use wisdom and discretion when considering how and when to approach parents about technology-related incidents that involve their children.

In most cases, it makes sense to gather and understand all of the relevant facts before contacting the parents. Make sure you contact parents in ways that do not compromise your investigation. Avoid accusing students without solid evidence to back up your claims. In some Tier 2 situations, principals may decide it makes sense to wait to contact parents until after formal findings have been rendered.

You can expect emotional responses from parents who may feel a need to protect their child. Be prepared to express empathy and assure them that their child will be treated fairly. When it's appropriate, do your best to help the parents and child feel safe and protected.

Finally, be careful about when and how you share sensitive information you have discovered to ensure student privacy rights.

Evaluate Incident

Investigations that involve many people—or incidents that involve more serious behaviors—may require follow-up interviews, careful cross checking of facts, and a willingness to reach out for help when it's needed.

Some students may need to be interviewed multiple times for consistency, clarity, and fact-checking. When you are satisfied that you have a firm grasp of all the relevant facts, you can proceed with your evaluation.

Continue to collect information and evaluate

Every investigation is unique, which means there is no one-size-fits-all formula. You should tailor your investigation to match the seriousness of the incident and the number of people involved.

Be willing to conduct follow-up interviews, cross-check various facts and claims, and bring in outside help when it makes sense.

This includes bringing in additional technical help to search school equipment and other digital evidence that you collected and preserved during your preliminary investigation. During this process, make sure you understand and honor privacy boundaries on private equipment (mobile phones and laptops).

For more details on conducting a fair, thorough, and effective investigation, see Learning Module B: How to Conduct an Investigation.

Engage with support groups

Your faculty and staff should be fully trained on your e-safety policies and be prepared to intervene to protect student safety. They also need to understand how school employees might become victims and how to take appropriate action.

This includes preparing them to receive information from students and parents and knowing what to do and what not to do with that information.

Every member of your staff should know how to handle concerns, manage evidence, and when to reach out to administration for a more involved investigation.

Consult stakeholders

As you investigate and deal with technology-related incidents, it's important to consult all of the stakeholders who can help you implement and support school actions to keep students safe. This includes:

- School administrators
- Teachers
- Network administrators and school IT professionals
- School nurses and counselors
- Media and digital literacy specialists
- School resource officers
- School law enforcement officers
- Community support groups
- Parents and students.

Parents and guardians can often provide valuable perspectives on relevant life events that factor into technology-related incidents, as well as on students' behavior before and after an event.

You can also invite community support groups to assist students who are dealing with specific issues. These groups include gang task forces, suicide support groups, support groups for kids with divorced parents, support groups for eating disorders, etc.

Take school action

After you receive input from all of the relevant stakeholders, you can make a fair, informed final decision and implement appropriate school actions.

When a student has been identified as an offender, in all but the most minor cases, the incident should be documented and placed in the student's file, and the student should be given at least a warning.

The file should be reviewed if the behavior is repeated or if the misconduct escalates. Repeat offenses can be addressed more effectively if the school has documented evidence of previous incidents.

Disciplinary actions may range from a warning to dismissal of a staff member or suspension of a student. As with all disciplinary actions, schools must be careful to follow the disciplinary protocols and due process standards documented in their formal policies.

Make sure you carefully and properly document every action. Investigation reports should be added to the appropriate student or faculty files. You should also write a School Action Report that summarizes the event and the school's response and include this report in the student or faculty member's files.

Finally, provide appropriate counseling and support wherever possible. Parents or guardians should be kept fully informed of the matter throughout the follow up process.

Follow up

You should conduct a comprehensive debriefing after every technology-related incident to analyze the results and explore areas for improvement.

It's helpful to break this vital post-incident exercise into three areas of focus for follow up questions and topics:

Support: Examine how well all of the involved parties were supported through the course of the investigation and determine if further counseling or additional support is required.

Audit: Explore how the incident was handled, including all of the processes and people that were used to support your students and staff. Carefully audit the process undertaken for each incident.

Evaluate: Evaluate all of the policies, practices, and procedures used to investigate and resolve the incident. Could the response be improved? Is there a need for further resources or training?

This follow-up component is a crucial component for maintaining high levels of digital citizenship and a positive school climate. With a thorough and effective follow-up, you can make sure that the technology-related incident was resolved to the satisfaction of all parties involved, including the offenders, victims, and bystanders.

Additional Resources:

Follow-Up Forms

Support

This first stage of the follow-up process involves understanding how all the involved parties were supported throughout the incident—and then determining if they need further support.

In most cases, this involves initiating formal follow-up reviews two, four, and twelve weeks after the incident has been resolved. The School Action Report form has a place to schedule these follow up dates, and they should also be entered into e-safety administrator's calendar. This graduated follow-up schedule provides opportunities to check back with the victims, perpetrators, and other bystanders. It does not include the formal internal review and evaluation of the incident management process.

The following questions may help guide your follow-up support efforts:

- As the e-safety committee or administrator, are we satisfied with the outcome of this incident?
- Are all parties concerned working well together?
- Are you currently in counseling? Do you feel the counseling is helpful?
- Do the student, parent, or staff involved in the incident require any additional counseling?
- If support is required for a parent, has the school checked in with the parent?
- In the event of suspensions, have students and parents received curriculum for learning at home during the suspension?

Next steps?

Audit

This phase involves a careful audit of the processes and procedures that were used to resolve an incident—and review the course of action taken by all stakeholders.

The e-safety administrator or e-safety committee should ask the following questions.

For school administrators and staff:

- How did we handle this incident? What did we do?
- Who was involved in the resolution? Were any outside agencies involved?
- At what point were they involved? Should they have been involved sooner?

- What actions resulted from the investigation? Were those actions in line with policies, practices, and procedures?
- Was the outcome satisfactory?
- At what point were parents involved?
- Next steps?

For victims and bystanders:

- Do you feel the incident is resolved?
- Do you have lingering fears?
- Are conditions improving?
- Do you feel supported by the school's administration and teachers?
- Are your parents aware of what happened? How did they find out? Have you discussed it with them further?

For other stakeholders:

- Why were you involved?
- How were you informed?

Do you have suggestions for our policies, practices, and procedures?

Evaluate

The Evaluate stage provides an opportunity for administrators to review the audit and implement responsive changes if necessary. It also provides an opportunity to reward good outcomes.

The following questions can help guide your final evaluation of the incident:

For victims and bystanders:

- Do you feel the incident is resolved?
- Do you have lingering fears?
- Are conditions improving?
- Do you feel supported by the school/teachers?
- Are your parents aware of what happened? (Keep family dynamics brief.) How did they find out? Have you discussed it with them further?

For other stakeholders:

- Why were you involved?
- How were you informed?
- Do you have suggestions for our policies, practices, and procedures?

Incident Response Flowchart

Incident Investigative Tools

Report Online Child Exploitation

Learning Modules Additional Resources Disclaimer

This website is funded through a grant from the Office of Juvenile Justice and Delinquency Prevention, Office of Justice Programs, U.S. Department of Justice. Neither the U.S. Department of Justice nor any of its components operate, control, are responsible for, or necessarily endorse, this website (including, without limitation, its content, technical infrastructure, and policies, and any services or tools provided).

Problems with the website?