If the incident involves criminal activity;

STOP!

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

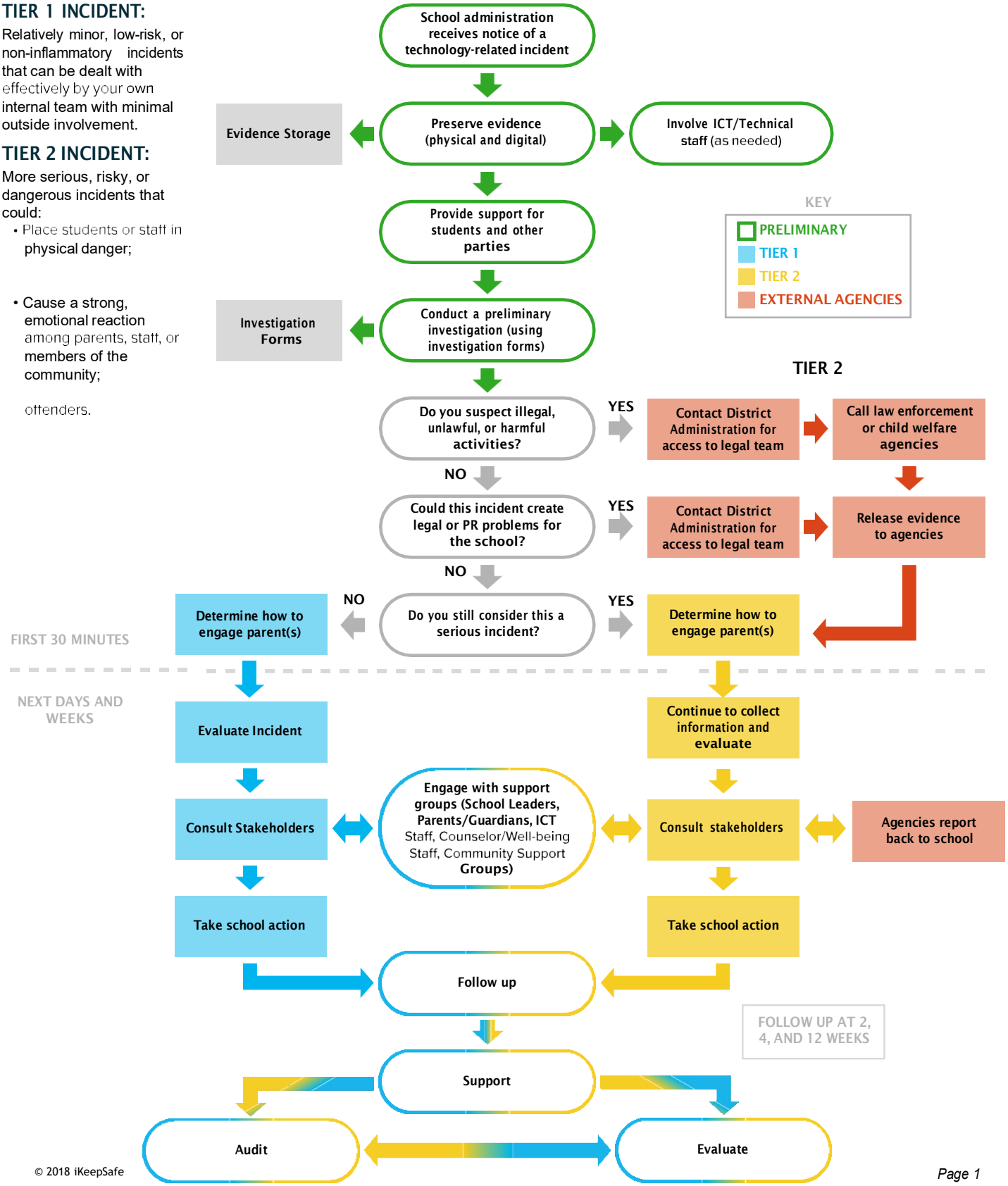
TIER 1 INCIDENT:

Relatively minor, low-risk, or non-inflammatory incidents that can be dealt with effectively by your own internal team with minimal outside involvement.

TIER 2 INCIDENT:

More serious, risky, or dangerous incidents that could:

- Place students or staff in physical danger;
- Cause a strong, emotional reaction among parents, staff, or members of the community;
- offenders.



If the incident involves criminal activity;

STOP!

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

FLOWCHART INSTRUCTIONS

The Incident Response Tool (IRT) will guide school administrators through the resolution of any technology related incident (involving digital information and technology). Based on your input, the IRT will produce a customized investigation plan to ensure the best possible outcome for victims, offenders, and bystanders. For best results preventing and resolving technology related incidents, administrators should take a coordinated approach that includes all stakeholders.

RESOLVING A SCHOOL TECHNOLOGY RELATED INCIDENT

SCHOOL ADMINISTRATION

With the support of the school e-safety committee, school administrators should take the lead in embedding digital citizenship into the culture of the school, designating a member of the administration (often the principal) with responsibility for managing an incident. This person identified here as the "e-safety administrator" should act as the central point of contact for all e-safety issues and digital citizenship concerns within the school. The e-safety administrator ensures that policies are current and adhered to, that breaches and abuse are monitored and reported, and that all faculty and staff receive relevant information about emerging issues.

Because digital communication has become entrenched in education, iKeepSafe recommends that the network/ ICT leader be a high-ranking district/regional or school administrator and that superintendents begin to hire district administrators who are technology savvy to handle the monitoring of school networks. If law enforcement is not involved with an investigation, schools should be prepared to handle digital forensics in a timely manner.

FACULTY/STAFF

Faculty and staff should know e-safety policies and be prepared to intervene for student safety. They also need to understand how school employees might become victims and how to take appropriate action. This includes being prepared to receive information from students and parents and knowing what to do and what not to do with that information, how to handle concerns, manage evidence, and when to reach out to administration for a more involved investigation.

TECHNICAL / INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT)

ICT staff will be helpful in developing policies and procedures for digital citizenship within the school or district/ region and will likely provide guidance and capture evidence during an investigation. The ICT staff is also likely to be a key reporter of incidents as they review filtering logs and manage networks. They will work closely with the e-safety administrator to conduct technical investigations and to improve the school network system to prevent future related incidents. Again, iKeepSafe recommends that the ICT staff be headed by a high-level technology savvy administrator.

PARENTS

Parents are often the reporters of incidents and need access to the e-safety coordinator or another way to report incidents. Expect reports to be submitted to the school front office, teachers, and to email addresses listed on the school website. Faculty and staff should be prepared to receive and process incidents, capturing relevant detail to be passed on to the e-safety administrator (based on your e-safety policy).

BYSTANDERS/OFFENDERS/VICTIMS

As bystanders, offenders, and victims of an incident, students will have many roles as incidents are handled. Training in digital citizenship, healthy and appropriate technology use, and reputation management will help minimize technology realted issues on campus and off.

INCIDENT OVERVIEW

Incidents will vary in scope and breadth. A technology related incident is any conflict or concern that arises through the use of digital technology, either with students or faculty and staff. Incidents may occur on-site or off-campus. School administrators should consider intervention in any incident that affects a students ability to focus and feel safe at school--whether it occurs on or off-campus.

Schools should consider any behavior outside of the Responsible Use Policy (RUP) to be an incident of concern and expect a variety of emotional responses from students with possibly a high emotional response from parents. Some incidents will impact the community or need the involvement of outside resources (school/district attorney, school counselors, nurse). Other incidents will be simple matters that resolve quickly between a few people. Incidents involving illegal or unlawful behavior will require police intervention and extreme care by administration and faculty. Proper training by school personnel will ensure the best possible outcomes for victims, bystanders, and perpetrators of a technology related incident and limit the school's liability.

The following technology related incidents show the breadth of situations that may arise. Many other possible technology related incidents could violate state law or school policy, including new problems that may require new policy:

- Alleged threats to students made off campus by students on social networking page.
- A student shares her password with another student who uses it and reads all of her emails and brags about it to other students.
- Racist comments posted on a student's social networking site by another student.
- Student couple breaks up and boy posts naked photo of girl on social networking site.
- Student harasses a teacher on social networking platform.
- Student takes picture of other students dressing in gym on mobile phone and sends images to victims in an attempt to blackmail for more images.
- Teacher "friends" student and makes inappropriate comments to student. This boundary invasion is further complicated when other students see the comments.
- Website is published with damaging information about a student or school staff member.
- Cyber-bullies taunt a suicidal student via text (on or off school grounds).
- Student posts suicidal comments on social networking site.
- Student posts video of party with students using illegal drugs or alcohol.
- Teacher sees student's screensaver on mobile phone contains CSAM or other illegal activity.
- Student posts a comment about his intent to harm students at school.
- Student posts a "jump in" fight on YouTube.
- Student cheats on test with mobile phone.
- Students anonymously post information about a widespread cheating epidemic at the school, which is unknown to administrators.
- Student hacks into school server and changes grades.
- Local gang recruits students on social media.
- Student is extremely tired at school and talks about World of Warcraft (or other online game).
- Student acts out video games on playground in a violent manner.

INCIDENT RESPONSE

Refer to the Incident Response Flow Chart in the event of an incident. The online flow chart gives a quick overview of a possible path toward successful resolution of a technology related incident. A mouse roll-over on the flow chart modules provides further information about each step and/or links to the full body of text below, including links to learning modules that will help administrators resolve an incident.

USE OF THE INCIDENT RESPONSE TOOL

An investigation will require a record of the incident that can be copied into the student/faculty files and used in resolution and follow up. The Incident Response Tool walks the e-safety administrator through an investigation and facilitates the interview process.

The e-safety administrator will determine how he/she is likely to conduct investigations and prepare accordingly:

For paper/pencil interview, gather:

- Copy of IRT Flowchart.
- Copy of Generic Investigation Forms or Customized Investigation Form produced through the online IRT.
- Clipboard or notebook.

For a digital record, gather:

- Bookmark to incident flowchart.
- Customized document with instructions and investigation question (produced by the IRT), ready to complete.

ALL FACULTY/STAFF AND STUDENTS ARE TRAINED ON THE E-SAFETY POLICY

Professional Development opportunities should be made available to staff and curriculum developed for students that incorporate digital citizenship into existing school culture and practice. An understanding of school policy will protect students and the school from inadvertent violation and increase the likelihood of best outcomes for all participants in an incident.

SCHOOL ADMINISTRATION IS NOTIFIED OF A TECHNOLOGY RELATED INCIDENT

Any technology related incident that occurs on campus is automatically an incident of concern. If an off-campus issue creates a substantial disruption at school, interferes with a student's right to learn in a secure environment, or poses a threat to a student or staff, the situation should be considered a school technology related incident.

PRESERVE EVIDENCE (PHYSICAL OR DIGITAL)

Proceed through this step with as much care as possible for the rights and dignity of all parties involved. The process of preserving evidence will cause stress and anxiety for some people. Once evidence is preserved, the e-safety coordinator should attend to the emotional needs of the people involved.

Before an investigation begins in earnest, the principal or e-safety coordinator should take immediate care to preserve any evidence that has materialized in the course of discovering the incident. Exercise extreme care when preserving evidence. An offender or other person may tamper or delete. Extreme care must be taken to avoid:

1. Contamination of evidence.
2. Possession of illegal or incriminating data on school or employee devices.

CONTAMINATION OF EVIDENCE:

An employee of a public school is legally an agent of the state and therefore subject to relevant privacy and search and seizure laws. The misstep of an administrator in collecting evidence (e.g. exploring files on a private mobile phone without probable cause) can lead to the evidence being thrown out if the incident goes to trial.
If illegal activity is suspected, the evidence will need to be preserved in its original form in a secure location to give to law enforcement, child welfare, or the school lawyer. 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.

POSSESSION IS INCRIMINATING

A school administrator, faculty, or staff should not, under any circumstance be in possession of or view child pornography, preferably termed CSAM-Child Sexual Abuse Material. CSAM is the visual representation of minors under the age of 18 engaged in sexual activity or the visual representation of minors engaging in lewd or erotic behavior designed to arouse the viewer's sexual interest. If you find CSAM or have a "reasonable suspicion" that it exists on a device, call the police immediately.

INSTRUCTIONS FOR PHYSICALLY PRESERVING EVIDENCE

NOTE: this relates to evidence in all incidents, except CSAM (See below for detail on handling evidence that may contain CSAM.)

Gather all digital data and copy to a secure memory device that can be locked in a secure cabinet. This backup will allow further investigation without damaging or compromising the original. Student mobile phones in question should be stored in an evidence bag (or Ziploc storage bag), and locked in a secure location (locked cabinet or desk).

Where school equipment is involved, a hard drive containing evidence may be copied in its entirety onto an external memory device specifically designated for the backup of evidence. If possible, have your network administrator or ICT staff help with the backup. This should be maintained for school records in the event that police are called in to confiscate the equipment. This hard drive should be locked in a secure location (desk or cabinet) until further investigation is possible. An evidence log, detailing everyone with access to the evidence, should be maintained throughout the process in the event that you have to certify that the evidence was not contaminated.

ACT QUICKLY:

Electronically stored information can be lost or destroyed very quickly, making further investigation more difficult and costly, if not impossible.

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. ICT staff (network administrators) and/or computer forensic specialists can help identify sources of electronically stored information and how they might be connected. Consider these:

- Hard drives of desktop computers, laptops, netbooks, and tablets/slates.
- Network servers (local 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 mobile phones can record incoming and outgoing calls, but also contain address books, calendars, voice and text messages, email, video and pictures.
- 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: When an incident has occurred offsite on the open Web, conduct a quick Web search for student profiles on popular social networking sites. Take screen shots and collect URLs, showing offending content or high risk behavior to be addressed.

CONFISCATE AND STORE EQUIPMENT AND MEDIA IN A SECURE LOCATION:

- Depending on the source of electronically stored information, different preservation techniques may be necessary to prevent documents from being destroyed or hidden data from being changed.
- 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.
- Portable media should be taken into custody and secured.
- 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. 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.

PREVENT UNAUTHORIZED ACCESS:

- Prevent faculty/staff from accessing data by blocking user ID numbers and remote access capability.
- Maintain hard copy documents where possible.

NOTE: **EVIDENCE OF CHILD SEXUAL ABUSE MATERIAL - CSAM (Child Pornography)**

If, at any point throughout this process, you have reasonable suspicion that CSAM exists on a computer or other electronic device, call law enforcement immediately. **DO NOT copy the hard drive or attempt to preserve digital data that might contain CSAM.** Leave the computer exactly as it is, (turn off the screen only if child pornography is on screen), and 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. Record this event in the school Incident Log. If no log exists, begin one with this incident.

See Learning Module B: How to Conduct an Investigation for more information, including instructions for preparing a secure location for evidence and how to collect evidence safely.

BRING IN TECHNICAL/ICT STAFF AS NEEDED

If the issue occurred on the school network or computer, call in the ICT staff to capture the evidence. Print physical evidence in the form of screen shots (e.g. website pages, file folder structures). Identify computer systems that were used, secure scene, and preserve trace evidence. Collect digital evidence that is needed. Document screen, system time, and network activity. Note any plainly visible cyber trails. Preserve contents of RAM if needed using approved tools and procedures. If the whole computer is needed, photograph, label, and document system details on collection form, disconnecting network, modem, and power cables. Collect needed software and peripherals, related documentation, removable media, passwords, etc. (Footnote: Casey)

STORAGE OF EVIDENCE

A plan for evidence storage should be prepared before an incident occurs. (See Learning Module A: Prepare for an Incident). Prepare a secure Preservation Hold that will ensure that evidence will not be contaminated or altered. Maintain 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 device is seized by a teacher after it is reported or observed to have inappropriate or illegal behavior.**

  It is important to understand the evanescent nature of the contents of a mobile devices; they can be password protected, encrypted and easily wiped from a remote location; as a result, the phone contents quickly become inaccessible forever.

  The teacher should, to the best of their abilities, document their observations, both in writing and if not illegal material, via photography/videography. If photography/videography is to be used, it is recommended not to use a personal cell phone or device, but the school should plan to have a dedicated camera for this purpose. If the password for the device is known, turn off the device and stored in a secure location. If the password for the device is not known, the device should be placed in "Airplane" mode and plugged into a power source. If possible, attempt to prevent the device from a locked screen and obtain additional guidance from an IT or law enforcement professional. All documentation should be secured.

- **Storage Scenario 2: A RUP/AUP violation occurs on a school owned computer.**

  It is important to understand that the computer screen most likely reflects information that is not stored on the computer's hard drive, but instead on a website or other online service. Turning off or powering down the computer may make some of all of this data irretrievable.

  If information is visible on the screen and shows evidence of a violation, all persons making these observations should document their observations both in writing and if not illegal material, via photography/videography. If photography/videography is to be used, if is recommended not to use a personal cell phone or device, but the school should plan to have a dedicated camera for this purpose. ICT staff should isolate the computer from the network and/or remove to a secure location until next steps can be determined; this might include the dumping of the random access memory (RAM) before turning off the computer and possibly making a copy of the internal hard drive while still powered on or after being powered off. All documentation should be secured.

ATTEND TO THE SUPPORT OF STUDENTS AND OTHER PARTIES

Determine the needs of the parties involved. Consider the emotional needs of victims, bystanders, and offenders. Offer counseling services where possible. To the extent possible, reestablish a safe environment for parties involved.

CONDUCT PRELIMINARY INVESTIGATION USING FORMS

After attending to the students and preserving the evidence, turn to the preliminary investigation of the incident. For more information, see Learning Module B: How to Conduct an Investigation.

Regardless of whether you are 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, 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 contaminating evidence.

Given the facts and circumstances of the particular case, determine the appropriate sequence of interviews that will be most effective in collecting other evidence. In sensitive situations, such as sexting, special consideration should be given for who should conduct the interview, particularly where the student is depicted in a compromising light. Administrators should expect that this student will be in extreme emotional distress due to possible circulation of a private image or communication. The investigation of this student should likely be performed by a school professional who has an excellent rapport with the student, such as a counselor, by a law enforcement official with specific training in working with sexual abuse victims, or a child protection worker. Every effort must be made to ensure that news of the incident is not spread.

INVESTIGATION FORMS

Consider how you would like your investigation to proceed. If possible, review the information in Learning Module B: How to Conduct an Investigation.

If you prefer using a clipboard, print out a complete set of the IRT Investigative Report Form, and store them on a clipboard (or folder) dedicated to this purpose. After collecting the information, a written summary should be added to faculty or student files.

Generic Investigation Forms will assist you in conducting a thorough investigation: General Information, Illegal Incident, Victim, Possible Offender, Bystander, and Possible Staff Offender forms.

TIER 1

DETERMINE HOW TO ENGAGE PARENT

Use discretion when considering how and when to approach parents. In general, administrators will want to gather all the relevant facts before contacting parents. Without compromising your investigation, consider when parents should be notified, taking care not to accuse a student without sufficient evidence to back up your claim. In Tier 2 scenarios, principals may decide it is best to wait until formal findings have been issued. Care should also be taken to ensure student privacy rights (Refer to school policy).

LOWER HALF OF FLOW CHART

The preceding events will likely occur in the first hour or less of the report of an incident. The ongoing investigation and followup will continue throughout that day and into the coming weeks.

EVALUATE INCIDENT

Investigations that involve many people or more serious incidents will require followup interviews, cross-checking facts, and reaching out for help when needed. Some students may need to be interviewed again for clarity and fact-checking. If you are satisfied that the incident is straightforward, proceed with evaluation.

CONSULT STAKEHOLDERS

Consult all stakeholders who might help you implement school actions and support those involved: other administrators, teachers, network administrator/ ICT staff, school nurse, school counselor/ wellbeing staff, media/ digital literacy specialist, school resource officer/law enforcement, parents, students involved. Parents and guardians may be able to give valuable perspective on relevant life events that might be factors in the incident as well as on the student's behavior before and after the event. Community support groups may be invited to assist students who are dealing with specific issues (eg gang task force, suicide support group, and support groups for kids with divorced parents, eating disorders, etc.).

Stakeholder groups to consider:

- District (Regional) Administrators
- School Administrators
- Educators
- Network Administrators
- School Nurse
- School Counselor/ Wellbeing Staff

- Media and/or Digital Literacy Specialist
- School Resource Officer/Law Enforcement
- Parent
- Youth

TAKE SCHOOL ACTION

With the input of stakeholders, make a final decision and implement school action. 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 if the school has evidence of previous incidents.

Disciplinary action may range from a warning to dismissal of a staff member or suspension of a student. As in all disciplinary instances, schools must be careful to follow the disciplinary protocols and due process standards in their policy. Take care that proper documentation occurs. Investigation reports should be entered in student/faculty files. Write a School Action Report that summarizes the event and the school's response, and include it in the student/faculty files.

Provide appropriate counseling and support where possible. Parents/guardians should be kept fully informed of the matter throughout followup.

TIER 2

Issues dealing with serious harm, illegal or unlawful activity, or that could create a significant PR problem for the school, are considered Tier 2 events and need immediate attention. Serious harm may include:

- Incitement (online coordination of a fight)
- Hate crimes
- Suicide threat
- Credible physical threat (might include physical, mental/emotional/psychological, or reputational harm to an individual)

Unlawful activity includes anything that could be prosecuted in certain contexts, such as harassment, sexual harassment, or slander.

IS THERE SUSPECTED SERIOUS HARM, ILLEGAL OR UNLAWFUL ACTIVITY --> YES

Any communication that shows the potential for serious harm or illegal/unlawful activity should be reported to local law enforcement immediately. You will likely want to notify district administration and consider bringing in legal counsel. Inappropriate employee electronic communications may contain speech that has the potential of violating various laws, including legal prohibitions against unlawful acts such as: discrimination, retaliation, harassment, defamation, network "hacking," or viewing and/or transmitting pornography.

WARNING: Discovery of CSAM or having a "reasonable suspicion" of CSAM on school equipment or within the school's network is a very serious situation, and should be reported to the police immediately. **DO NOT download, print, or otherwise preserve any data containing CSAM**, as this may implicate you or other school employees in the crime. Leave the computer exactly as it is, (turn off the screen only if CSAM 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. Record this event in the school Incident Log. If no log exists, begin one with this incident.

If illegal behavior by a student or staff member is suspected, the school has a duty to consult with the police at the earliest opportunity, preserving any potential evidence for school records and to hand over to the police. This may also involve reporting to other outside agencies.

MANDATORY REPORTING TIMELINES

Take care to report illegal activity in a timely manner. Most states have mandatory reporting guidelines that require a school to report child abuse or neglect "**immediately or as soon as is practicably possible** by telephone". Be sure to follow your State's Mandated Reporter Law.

Schools are also required to **"promptly report"** when an employee of a school or district **"is attacked, assaulted, or physically threatened by any pupil."** This applies in most states.

COULD THIS INCIDENT BECOME A LEGAL OR PR PROBLEM FOR THE SCHOOL? --->YES

Legal and PR problems (eg potential litigation, negative media attention, or a united community force against the school) are serious issues for a district, and are treated here as Tier 2 events. In these situations, the school attorney and district administration should be notified immediately. These items will follow Tier 2 on the flow chart.

DO YOU STILL CONSIDER THIS A SERIOUS INCIDENT? (EG, REPEAT OFFENDER) ---> YES

After illegal issues and possible PR problems for the schools, there are still many issues that will fall into Tier 2 as incidents that need serious attention. Incidents involving repeat offenders or youths at risk for future crimes may be considered for Tier 2. While not illegal, technology related incidents such as plagiarism and cheating are serious problems that schools and universities are trying to correct and may fall into your school's classification of "serious incident," particularly for repeat offenders.

CONTACT DISTRICT ADMINISTRATION/SCHOOL ATTORNEY

If you suspect the possibility of serious harm or illegal/unlawful activity, call your district/regional attorney as you contact law enforcement. If the incident might be made public through the media, cause a disruption to the school climate, or result in possible litigation (harassment, discrimination, etc.) contact district level administration is recommended and request legal counsel. In many districts the only authorized contact with counsel is through a district administrator. A school attorney and district administration will provide support for managing a legal or PR problem.

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. For example:

- Evidence that someone on or off campus is in danger of serious harm (e.g., plans for a gang fight, plans to hurt someone).
- 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 CSAM or have a "reasonable suspicion" of CSAM, call police immediately. Do not copy, preserve, or otherwise store digital data that might contain CSAM. Work closely with these officials to coordinate next steps, as they may need to collect evidence from the school. Where possible and legal to do so, retain as much evidence as you can to support your internal investigation as you may not have access to surrendered evidence again.

A school must continue its investigation and document evidence even if police take over in the investigation.
A good working relationship with law enforcement where both parties are inclined to share information

will produce the best results for both the school and police. This information is essential if the school needs to proceed with a termination hearing which may be difficult if a criminal case failed to convict based on a technicality, but the school seeks dismissal.

If there is suspicion of any kind of abuse of a student by anyone, contact a child welfare agency concurrent with calling law enforcement. Most states have mandatory reporting guidelines for reporting child abuse or neglect. A reasonable suspicion will obligate you by law to report to the agencies, you do not need a burden of proof, only a "reasonable suspicion."

RELEASE EVIDENCE TO AGENCIES

Any preserved evidence should be shared with law enforcement or any other agency that assumes jurisdiction over the investigation. Where possible and legal to do so, retain as much evidence as you can to support your internal investigation as you may not have access to surrendered evidence again.

DETERMINE HOW TO ENGAGE PARENTS

Use discretion when considering how and when to approach parents. In general, administrators will want to have gathered all the relevant facts before contacting parents. Without compromising your investigation, consider when parents should be notified, taking care not to accuse a student without sufficient evidence to back up your claim. In Tier 2 scenarios, principals may decide it is best to wait until formal findings have been rendered.

It is reasonable to expect a wide range of 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 or helped to feel safe, depending on the circumstance.

Always exercise caution when sharing information discovered in the investigation to ensure student privacy rights.

CONTINUE INVESTIGATION AND EVALUATE INCIDENT

Each investigation is unique and fact-specific, so one formula will not always apply to every situation. Investigations that involve many people or more serious incidents will require further investigation with followup interviews, cross-checking facts, and reaching out for help when needed. Some students may need to be interviewed again for clarity and fact-checking. Get technical help to search school equipment and other digital evidence, preserved during the preliminary investigation, taking care not to over-reach privacy boundaries on private equipment (mobile phones and laptops).

If your preliminary investigation yields information that is particularly inflammatory or possibly criminal, call your school attorney, or consider hiring an independent third party to conduct a full investigation. For help getting the most out of your investigations, see Learning Module B: How to Conduct an Investigation.

The following instruction will allow you to approach each investigation thoroughly and effectively so that if your investigation is challenged, you will be able to explain how you gathered and weighed the relevant evidence and met your burden of proof when you made a decision and took a particular action.

GUIDELINES FOR EVALUATING AN INCIDENT

Review all of the evidence gathered:

1. Review all of the relevant documents, tangible evidence, and your interview notes.
2. Review all of the applicable policies, regulations or other procedures again.
3. If you've missed anything or you forgot to ask important questions, go back and ask more questions.
4. If you can't understand your notes, go back and ask clarifying questions.
5. If you are confused by a respondent's testimony, go back and ask clarifying questions.

6. In a disputed matter, if you cannot decide who appears to be truthful and who appears to be deceptive, you may want to conduct another interview with each person.

Weigh evidence for each allegation.

Evaluate all the evidence and make a determination. It is possible that you will make a mistake and find in favor of the wrong evidence. However, if you performed a prompt, thorough, and effective investigation, evaluated all the evidence in good faith, and reached a reasonable conclusion, it is likely your mistake will not cause liability.

Administrators are governed by a "preponderance of evidence" standard. That means you are looking to see if a simple majority (50% plus a feather) of the evidence weighs more on one side. Weigh the evidence, including testimony from eye-witnesses, corroborating testimony, circumstantial evidence, and credibility evidence. If the evidence is not in dispute, it is easy to "weigh" the evidence, because it all leans to one side. NOTE:

- A hunch or speculation is insufficient evidence.
- Hearsay evidence may have some weight only if it supports direct evidence.
- If the evidence is in dispute, you must look at all the evidence closely and determine which evidence is most persuasive. Be prepared to explain why some evidence was more persuasive than other evidence.

Make a factual finding for each allegation.

A factual finding is a conclusion about what happened, based on the preponderance of the evidence.

Review all factual findings to determine if a violation of law or policy has occurred.

Prepare a summary report.

Some schools create a summary or executive report that can be given to the school or district governing board that could be released under a Public Records Act request. Typically, such a report does not include any witness statements or other evidence. A summary or executive report may include the allegations, the findings, the conclusions reached, and general recommendations based upon the conclusions. Consult legal counsel as to how to proceed further in this regard, especially before releasing any information to the public regarding the investigation.

Once you feel comfortable that the relevant facts are gathered, evaluate the situation. Consider which stakeholders might help deciding and implementing school actions and supporting those involved (school counselor, ICT staff, media specialist, etc.) Make arrangements to meet as a group if possible or talk to them individually.

FOLLOW UP

In all instances, a comprehensive debriefing should occur after the incident to maximize what can be learned. The three sections (Audit, Support, Evaluate) create areas of focus for followup questions and topics that should be addressed before an incident is laid to rest in student and school files.

- Support: Understand how the involved parties were supported, and determine if further counseling or other support is required?
- Audit: Gather a picture of how the incident was handled--all processes and people gathered to be the network of support for the students and staff. Audit the process undertaken for each incident.
- Evaluate: Consider all policies, practices and procedures. Could the response be improved? Is there a need for further resources and or training?

The follow up to an incident is a very important component of maintaining a high level of digital citizenship and positive school climate. The follow up ensures that a technology related incident was resolved to the satisfaction of all parties involved: offenders, victims, and bystanders.

SUPPORT

Understand how the involved parties were supported, and determine if they need further support. As an incident reaches resolution, plans should be made to initiate the follow up process at two, four, and twelve weeks following the resolution of the incident. The "School Action Report" has a place to record anticipated followup dates. These dates should also be entered into the calendar of the e-safety administrator (or representative responsible for followup). This graduated followup is specifically designed to check back with the victim, perpetrator, and any bystanders of an incident and does not include internal review and evaluation of the incident management process.

The following questions may help provide followup support: (Print Supplemental Report Form here).

- As the e-safety committee/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 it's helpful?
- Is further counseling required? Any other support required by the student, parent, staff involved?
- If support is required for parent, has the school checked in with the parent?
- [In the event of suspensions] Have you received curriculum for learning at home during the suspension.
- Next steps?

The internal followup (REVIEW and EVALUATE), will identify where the incident management succeeded and where it might be improved.

AUDIT

The purpose of this section is to audit the process undertaken for resolving each incident and review the course of action taken by all stakeholders. The e-safety administrator or e-safety committee should ask the following questions: (Print Supplemental Report Form here).

- How did we handle this incident? What did we do?
- Who was involved in the resolution? Any outside agencies?
- At what point were they involved? Was it soon enough?
- What actions resulted? Was what they did in line with policies, practices, and procedures?
- Was the outcome satisfactory?
- At what point were parents involved?
- Next steps?

Ask the 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?
- Gather a quick snapshot from stakeholders involved?
    - Why were you involved?
    - How were you informed?
    - Do you have suggestions for our policies, practices, and procedures?
    - Next steps?

EVALUATE

This section will help administrators review the audit and implement responsive changes where necessary. It is also an opportunity to reward good outcomes. (Print Supplemental Report Form here).

- 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?
- Gather a quick snapshot from stakeholders involved?
  - Why were you involved?
  - How were you informed
  - Do you have suggestions for our policies, practices, and procedures?