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

LEARNING MODULE B
How to Conduct 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.

Here are some questions to consider:

- Do you feel adequately trained to conduct a prompt, thorough and effective investigation into technology-related incidents?
- Do you know the steps you should take to preserve evidence?
- Do you know when you are required to report a technology-related incident, and to whom you should report?

This learning module will prepare administrators to thoroughly gather the facts so they can confidently make careful decisions, particularly as new laws relating to technology use continue to emerge and evolve. These directions encourage the investigator to uncover all the relevant facts, not just the facts that may support a certain outcome.

LEGAL REQUIREMENTS FOR INVESTIGATIONS

As a general rule, all investigations should be prompt, thorough and effective. The investigator should gather evidence so that he or she can make a decision as to what occurred. We call these "findings of fact." If there is a dispute in the evidence, the investigator should rely on a preponderance of evidence to determine what occurred.

A preponderance of evidence is where one side of the evidence weighs heavier than the other. For example, 50% plus a feather would constitute a preponderance of the evidence. Another way to state the standard is, "More likely than not, the incident occurred" or "more likely than not the incident did not occur." When an investigator uses this standard to gather and weigh the evidence to determine the "Findings of Fact," the school can rely on the factual findings to decide what disciplinary or remedial action (if any) should be taken.

Administrators should be able to answer affirmatively to the following

1. Did you act in good faith, making your decision?
2. Did your decision follow an investigation that was appropriate under the circumstances?
3. Did you have reasonable grounds for believing that misconduct took place?

State laws provide further guidance for investigations in employer/employee guidelines. Some examples include:

- Investigations should be conducted by written policy, which proscribes how the investigation should be performed.
- The investigation should be performed by a well-trained, objective investigator(s).
- The investigation should be performed as soon as possible after the allegations are known, and it should be conducted in a confidential manner.
- The investigation should be performed in a manner which provides all witnesses, the alleged victim and the alleged accused with the opportunity to be fully and fairly heard.
- The investigation results should be documented.

The following will help schools prepare for, investigate, and respond to technology-related incidents.

EDUCATE USERS ABOUT TECHNOLOGY USE AND CONSEQUENCES ASSOCIATED WITH MISUSE

Develop, disseminate, and adhere to technology use policies, including those in:

1. Board Policies and Administrative Regulations/Procedures
2. Collective Bargaining Agreements (employees)
3. Student Handbooks (students)
4. Responsible Use Policies / Acceptable Use Agreements (RUP/AUP)
    a. Identify clear consequences associated with misuse
    b. Obtain signed agreements
    c. Make agreements age-appropriate
    d. Combing these agreements with training
    e. Incorporate school and educational philosophy into agreements
    f. Consider a collaborative approach when developing agreements

DETERMINE THE APPROPRIATE INVESTIGATOR

In general, the principal or other administrator conducts an investigation. Identify school personnel who will be involved in investigating technology-related incidents (e.g., administration, information technology personnel, school resource officer). The investigator should be:

1. Trained and qualified
2. Available
3. Impartial and unbiased
    a. Can keep an open mind while gathering the evidence, even if he or she knows some or all of the participants.
        i. Can avoid drawing conclusions until all relevant information is gathered.
        ii. Will be thorough
        iii. Demonstrates appropriate behavior
            1. Is trustworthy and will maintain confidentiality
            2. Does not have an extreme personality trait, such as being a “pushover” or a “jerk.” Extreme personalities can affect the ability to accurately judge credibility.
            3. Can avoid politics or other intervening issues and stick to the facts of the complaint.

Consult legal counsel before finalizing policies and agreements.

PLAN INVESTIGATION

1. Promptly review a complaint or report of technology misuse.
2. Conduct preliminary investigation: gather basic facts
    a. Who is involved (e.g., student/employee, minor/adult)?
    b. What happened (e.g., did someone send, receive, access, or post an inappropriate electronic communication)?
        i. What is the nature and extent of the communication (e.g., photo, video, email, or text and threat, crime, harassment, discrimination)? *NOTE: If the communication may constitute child pornography*

(e.g., frontal nudity of a minor student), consider enlisting assistance from the school resource officer before viewing

ii. What equipment was used (e.g. personal or school technology)

c. Where did the communication originate and where was it distributed (e.g., was it sent, received, or accessed on campus or with school resources)?

d. When did the incident occur (e.g., date, time, before/after school, during instructional time)?

e. Why (e.g., what were the possible motives behind the communication)?

f. Other:

i. Document any admissions.

ii. Develop plan for further investigation.

iii. Consider options for searching, preserving, and obtaining evidence.

iv. Contact parent/guardian as appropriate.

REVIEW APPLICABLE POLICIES AND RULES

- Guidelines: What policy, regulations or procedure apply or guide me in responding to the alleged conduct?
- Agreements: Do any applicable collective bargaining agreements touch on the alleged conduct? For example, does the certificated CBA contain an article regarding technology use?
- Identify Laws: What laws and/or policies may apply to this complaint? For example, does the conduct implicate child pornography, a violation of sexual harassment policies, discrimination on the basis of a protected status, general unprofessional conduct, misuse of employer property, or violation of a criminal law, etc?
- Review Laws: Do I understand the relevant laws so that I know what to look for when I'm looking at the evidence and interviewing the complainant (if any), witnesses and respondent?
- Paid Administrative Leave (employees): Does the complaint allege any health and safety issues that warrant paid administrative leave for the respondent pending the investigation?

NOTE:

- *Paid administrative leave is not used for disciplinary purposes.*
- *Notification of paid administrative leave should be placed in writing and contain instructions to the respondent regarding availability and expectations during the investigation.*

CONSIDER USING LEGAL COUNSEL OR AN OUTSIDE INVESTIGATOR WHEN:

1. Complicated legal issues or allegations arise.
2. Complicated chain of custody requirements for the evidence are present.
3. The investigation becomes complex, involving numerous complainants, witnesses and/or respondents.
4. You need help identifying or understanding the elements of an applicable law.
5. The complainant, respondent or witnesses have hired an attorney to represent them during the investigation.

BRING IN COMPUTER EXPERTS WHEN NECESSARY

In extreme cases, when misuse of technology, inappropriate electronic communications, or the need to gather electronically stored information arises, you may need to rely on information technology "experts" to identify,

preserve, collect, and depending on the circumstances, analyze the electronically stored information without damaging any digital evidence. Contact your district or school attorney for help choosing a qualified expert. The following information may useful as you make this decision.

1. Possible experts include:

    a. An information technology manager or employee already on staff: Although this may appear to be the more cost-effective option, consider whether the individual is well-trained in handling and preserving the electronic evidence and suited to handling cross-examination should his or her testimony concerning the evidence preservation and collection be needed in the future.

    b. An outside computer forensic expert: This option will likely cost more, but the preservation and collection of evidence will more likely withstand scrutiny in the event of a challenge.

    c. Law enforcement: If there is concern that the technology use violated the law, such as access to child pornography, law enforcement should be contacted immediately. In such instances, law enforcement will confiscate the equipment and undertake its own forensic analysis.

2. Confirm that your computer forensic expert (whether in-house or retained from outside) is:

    a. Certified Forensic Examiner

    b. Has experience offering live and declaratory expert witness testimony at trial and has not been disqualified as an expert. Has more than five years of 'hands on' forensic collection and examination experience with references.

    c. Has performed forensics on local machines, PDAs, servers, and has worked with slack and unallocated space

    d. Can provide a (redacted) analysis report (i.e., deleted data)

3. Expect the expert to:

    a. Charge between $250 and $350 per hour

    b. Require conflict checks and questionnaires to be completed before engaging.