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

LEARNING MODULE F

The Whole School Approach to Data Privacy

Education technology and cloud-based services offer important new opportunities and efficiencies for schools. From programs that create streamlined bus routes to interactive homework programs that track a student's progress to a portal that allows parents to get real-time information about their child's tests and assignments, educational technology can offer tremendous insight into a student's educational needs, innovative learning techniques, stronger communication with parents and an ease on administrative burdens. Along with these benefits, however, come serious questions about how best to protect student privacy.

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.

The first step to increase the whole school's confidence in the privacy of student data is to implement a comprehensive privacy program that will:

- Identify and minimize risks of a privacy mishap
- Document an incident response plan
- Keep policies up-to-date in light of changing technologies and laws
- Train employees about their privacy responsibilities
- Educate students and parents about privacy issues

A privacy assessment of existing technologies used in schools, preferably one conducted by an independent third party, can provide necessary information and direction for school systems seeking to enhance their data privacy policies and practices.

A privacy assessment will identify:

- Risks, gaps in policy, and areas where policies are misunderstood or are not being followed
- Policies that need to be updated in light of new laws and technologies
- Types of data collected by various departments, how they use it, who has access to it and how securely it is maintained
- Student data collected through technology used by the school, in and outside of the classroom

A school e-safety committee and a privacy point person should be established to review the result of the assessment, monitor ongoing compliance, recommend policy and practice changes and manage privacy-related communications.

A school system's policies should articulate a set of privacy practices that a school will follow, such as providing notice to people (students, parents, employees, etc.) regarding the data collected about them. The policies should also establish rules for key practices, such as maintaining confidentiality, security and integrity of the data it holds, identifying circumstances when the school will disclose data without consent, and how the school will communicate future policy changes. The policy should be drafted in language that is clear and easily understood by all of the intended audiences. In addition, a school should train and certify all employees on the policies.

As noted above, privacy training is instrumental to the effectiveness of a privacy program. Consistent with the whole school approach, privacy training and education should be provided to:

1. **Students.** Educating students about protecting their online privacy and becoming savvy digital citizens is essential to help them understand the consequences of their activity online. It will help them protect themselves and learn to manage key parts of their lives in the digital age.
2. **Parents.** Educating parents about technology being used in the classroom and their rights around student data privacy and record access is also of vital importance. In addition, parents need to know the challenges and opportunities that technology provides their children. And they need to know what to do to protect themselves and their children.
3. **Educators.** Educators will benefit greatly by being more informed about data privacy and security regulations and norms, the pitfalls that can happen when technology is not assessed properly before being introduced into the classroom, and perils that they and their students may face around technology incidents. Educators also need to be trained about how to deal with incidents such as cyberbullying harassment and sexting, which can invade the classroom through inappropriate use of technology.
4. **Administrators (including network administrators).** Administrators will benefit by improving their skills and competencies around student privacy. Administrators need to know the requirements and boundaries of regulations, what policies and procedures should be in place before technology is introduced into a school, protocols that should be followed if an incident occurs and how to ensure the community can have confidence in the services and technologies utilized by their schools.