

Creating Healthy Digital Environments for Students

toolkits

Data privacy is not only an issue of digital learning systems, third-party providers, and legislation. It's also an issue of digital citizenship and common sense.

Data privacy is not only an issue of digital learning systems, third-party providers, and legislation. It's also an issue of digital citizenship and common sense.

Digital citizenship is the practice of ethical and appropriate behavior when utilizing digital devices and online environments. Training staff and students in data privacy and healthy digital practices is essential to both preventing incidents and minimizing the damage of a potential technology-based incident, such as cyberbullying or sexting.

For students, this means exhibiting kind and sensible behavior when using technology and when communicating or collaborating with other students or faculty with digital devices. This requires a practical understanding of rights, restrictions, and standards (both ethical and legal), as well as strategies for personal protection and information security.

For faculty, this means being well versed in popular technology and digital communications, online behaviors, acceptable use, policies, and possible areas of infraction (and subsequent consequences) with the goal being safe and responsible school-wide collaboration and communication.

One proactive step that schools can take to prevent incidents in the first place is to establish through open discussion what acceptable digital etiquette looks like. In this way school administrators can establish a culture of digital citizenship and open communication while ensuring that policies are both relevant and adhered to. Another way to “walk the walk” is by forming a dedicated group devoted to digital citizenship matters. This group should meet regularly and focus on ways that your school or district can maintain optimum cyber-safety practices. Assigning clear roles and responsibilities will make this group more useful, as well as creating an actionable digital safety curriculum that can help to educate faculty, students, and parents by clarifying rights and responsibilities, responsible use, and cyberbullying.

Despite a school or district's best efforts, cyber incidents can happen—and they do. But the test of a school's mettle comes in how these incidents are dealt with. This takes effective and easy reporting systems, such as trusted staff members, anonymous phone lines, email reporting, where students can report incidents without fear of retaliation. Effective response also requires staff skilled in incident management, conducting interviews, and interacting with all parties, including local authorities if necessary.

Your IT staff can also provide guidance in the development of response procedures (e.g., utilizing filtering logs). These incidents should help feed measures to improve school networks and digital safety procedures to reduce the likelihood of future transgressions.