FACTS
A nelnet Company

Top Tips for Keeping School Information Safe

Whether you're working from home or in the office, cybersecurity basics can go a long way to protect you and your school's data. Working for a school means handling sensitive paperwork and electronic records, in addition to accessing a wide variety of data. Much of that data can be incredibly sensitive, including confidential, personal, health, and financial information. Both the data owners (parents and faculty) and school leadership rightfully expect that this sensitive data will be managed safely and securely.

With the evolution of modern environments and the rise of cybersecurity threats, however, it seems like keeping sensitive information safe proves more challenging every year. What can schools do to better protect themselves? Here are some of our top tips:

Top takeaways:

- Prioritize assessing the equipment that faculty and staff are using to perform their work. Do they have a school-provided laptop they can work on? Do they have access to a secure network if working from home?
- Make sure staff members that are working with confidential or personal information are using a dedicated workspace and protecting it well.

Additional resources:
Security through Education provides advice on data protection for schools

EDUCAUSE provides guidance for data classification

ATLIS provides cybersecurity recommendations for schools

Institute a data classification policy

Provide categories for classifying and labeling sensitive data and documents to ensure they are protected properly depending on their classification. For example, financial information could require encryption and limited access, while a school newsletter may be public information. Data classification can be based on legal requirements, value of the data to the school, criticality, sensitivity, or whether or not the information is determined to be public.

Control network security and access

Where sensitive information was once protected by secure, on-campus networks, it is now being worked on and accessed at home or in other remote workspaces. It's essential to keep all computers and accounts secure and in good working order. When possible, schools should utilize VPN access for an additional layer of network security. You'll also want to communicate to WFH staff the importance of using Wi-Fi networks that are as secure as possible - ideally private, home networks using strong passwords.

Maintain a clean desk policy

When kitchen tables become work desks and spare corners become offices, it can be more difficult to maintain data integrity and physical security. If an employee doesn't have access to a locked room, file cabinet, or briefcase to keep physical files safe, they should do their best to keep all work files together in a safe place and set boundaries with family members or roommates. Remind employees not to take or send photos of their remote workspace in case they've accidentally left passwords or documents with sensitive information out in the open.

Increase awareness and training

Providing training for all faculty and staff on data classification, data protection, and staff requirements on at least an annual basis is essential. For staff working in departments like admissions, financial aid, or human resources, having information open and readily accessible is a potential security threat. Keeping computers locked when staff are away from their desks, having strong password requirements school-wide, and reinforcing data storage and transmission policies are critical steps to ensuring school security.