Mobile Device Safety Tips for Teachers

As technology and mobile devices continue to make their way into classrooms, there are things teachers should be aware of to better protect themselves, their students and their data.

Products such as netbooks, smartphones and tablet devices not only help keep students engaged in the classroom, but they also serve as effective learning tools. These devices are great for conducting online research and collaborating and communicating with others. However if not monitored and managed properly, these devices can expose users to all kinds of security threats and/or the risk of data loss.

We've put together a list of our top tips for teachers to secure mobile devices so everyone stays safe.

User Names and Passwords: First and foremost, it's important to make sure user names and passwords are set up on devices so they are not easy to guess. Using a combination of upper and lower case letters, numbers and symbols will help make passwords more secure. Furthermore, making sure that any sensitive data that's on the device is password protected is key to ensuring that confidential information doesn't end up in the wrong hands — literally.

Backup and Recovery: It's important to remember that data on these devices should be backed up on a regular basis. Backup and recovery solutions enable faster system restores and also ensure mission-critical data is immediately accessible if an unfortunate event were to occur. If you are unsure whether your device has a backup hardware or software solution installed, or if you are unsure how to use it, ask your IT administrator for help. Additionally, regularly performing software and security updates will help protect information and devices.

Securing Mobile Devices: In the classroom, students may be encouraged to use social media Web sites such as Twitter and Facebook to engage with their peers. Taking pictures and posting information on the Web has never been easier now that the majority of mobile devices have built-in cameras and are able to connect to the Internet. As some devices have a geotagging function, you may want to consider disabling it since photos and videos can be tagged with latitude and longitude coordinates that illustrate where they were taken.

Be Wary of Public Wi-Fi: If your school or class accesses the Internet over a public Wi-Fi connection, you should exercise caution. Avoiding Web sites that request personal information and limiting file sharing to only authorized users will help safeguard the integrity of the device and any information that's on it.

Depending on what devices are accessible and allowed in schools, students may use smartphones, tablets, PCs or laptops. With a range of technology devices to choose from, it is critical to make sure students know the risks associated with using Internet-enabled devices. Cautioning your class to only

open e-mails and attachments from people they know and trusted sources can help reduce the risk of fraud and identity theft.

In addition to these tips, you may also want to consider coming up with a list of mobile device safety rules for your students to follow in the classroom. Being made aware of what type of content is appropriate (and not) for posting on the Internet is the first step to ensuring they remain safe both in and out of school.

Teaching students how to use mobile devices safely in the classroom can not only help mitigate security risks, but will also ensure these devices can be used to their full potential, turning them into learning enablers, instead of detractors.

Follow Teaching with Technology on Twitter (@teaching_w_tech).

Find more IT resources and free tools for teachers on the Teaching with Technology Facebook Page.

CDW Canada is a leading provider of technology solutions and a trusted advisor for educational institutions. For more information, visit http://www.cdw.ca/. To learn more about the Teaching with Technology Story Contest and Sweepstakes, visit http://www.teachingwithtechnology.ca/.