

Privacy and Security Tips for Educators

CYBERSECURITY AND PRIVACY | EDUCATION | APRIL 3, 2020



Christina M. Gagnier

VISIT THE CARLTON FIELDS CORONAVIRUS RESOURCE CENTER 

Download Printable Handout

As education and communication with students has transitioned online, the privacy and security of educators and the information that they are sharing online becomes ever more important. The following privacy and security tips can help educators and their students stay safe while distance learning and communicating using online tools.

Tip #1: Check Your Wi-Fi Network

Make sure to use a secure Wi-Fi network. Open Wi-Fi networks can lead to the information shared being compromised.

- Make sure at-home Wi-Fi networks are password protected.
- If it is not clear how to secure a currently open network, reach out to school or district IT or technical support to solicit help in how to do so.
- Using a secure network is important since educators deal with student information and education records, which are protected under the Family Educational Rights and Privacy Act (FERPA) and, in some cases, may be working with sensitive information regarding a student's abilities and learning.

Tip for Schools and Districts: Have IT personnel prepare an email for employees providing step-by-step guidance on how to secure a home Wi-Fi network.

Tip #2: Think Before You Click

Email has become essential to student and parent communication. This influx of communication becomes ripe ground for scammers seeking to cause harm and engage in malicious behavior.

- *Ask yourself: Is something just "off" about an email? If so, check for the following:*
 - Are you receiving a communication with shortened or cutoff links?
 - Is the email address an address that you recognize? Is it similar to a recognized address, but just a few letters or numbers off?
 - Hover over links so that the full link can be viewed.

Tip #3: Change and Update Your Passwords

Passwords should be changed and updated frequently. Create different passwords for different accounts.

- Do not have a universal username and password. While it may be easier to remember, it will lead to increased risk exposure.

Tip #4: Use a School-Issued Device When Engaging in School-Related Business

Educators should make sure to use their school-issued device when engaging in distance learning and communication with students. Files should not be moved onto a personal computer. School-issued devices are likely being supported by school or district IT teams who may be installing updates, running antivirus scans, and blocking certain websites that may be threats. Using a personal device could be putting students and the school at risk.

Tip #5: Check Your Privacy Settings

In the transition to distance learning, educators are using new software tools. Each new software tool should be reviewed, and the privacy settings should be customized in each tool.

With videoconference platforms, like Zoom, passwords should be used and shared with students and other educators. Hosting meetings without password protection may lead to uninvited parties joining an online classroom.

Tip #6: Cover Your Camera

Videoconference platforms that are now being employed use the camera in a computer or tablet for interactions with students. When a camera is not being used, it should be covered up.

- Use a simple “hack,” such as a Post-it note, to cover up a camera, or find a camera cover, which can be purchased online and affixed over a camera.

Tip #7: Back Up Documents and Information

Educators should make sure that they are using a secure solution to back up their data on a daily basis. Student information should not be left on personal hard drives or USB drives.

Tip for Schools and Districts: Work with legal counsel to find a cloud data storage solution that has created enterprise-level products using best-of-breed data security standards. Create a quick training for employees on how to use it and remind employees daily to back data up.

©2021 Carlton Fields, P.A. Carlton Fields practices law in California through Carlton Fields, LLP. Carlton Fields publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information and educational purposes only, and should not be relied on as if it were advice about a particular fact situation. The distribution of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship with Carlton Fields. This publication may not be quoted or referred to in any other publication or proceeding without the prior written consent of the firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our Contact Us form via the link below. The views set forth herein are the personal views of the author and do not necessarily reflect those of the firm. This site may contain hypertext links to information created and maintained by other entities. Carlton Fields does not control or guarantee the accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.