Technology Security Checklist for Teachers

TECHNOLOGY SECURITY CHECKLIST FOR TEACHERS

Technology has an increasing presence in schools and classrooms. However, these tools also pose security risks to sensitive data. Teachers play an important role in protecting student privacy. Below is a checklist of security procedures to follow when using school-related technology.

General Guidelines

- ❑ Do not share passwords for school accounts with anyone, including other staff or family members.
- ❑ Use different passwords for your school accounts than you do for personal accounts.
- ❑ Avoid connecting to the Internet through wireless networks (WiFi) that are not password protected.
- ❑ Immediately report to the administration any suspicious activity involving or affecting technology related to school work, school accounts, or student data.

Using Computers, Tablets, and Other Devices

When you are using school-owned equipment:

- ❑ Ask the administration whether your district or school has a policy about using school-owned computers, tablets, or other devices.
- ❑ Log out of accounts and close browsers and programs whenever you finish using a program.
- ❑ Password-protect, lock, or otherwise secure all computers and devices when not in use.
- ❑ Immediately report lost or stolen devices to the administration.

When you are using your own equipment:

- ❑ Ask the administration whether your district or school has a policy about bringing your own computer, tablet, or other device to school or using your own device for school purposes.
- ❑ Ask the administration if approval is necessary prior to using your own computer or other device in the classroom or to access student data.
- ❑ Install anti-virus software on the device before using it on the school network or to access school accounts; below are links to free anti-virus programs available for download:
  - ➢ Avast Free Antivirus: http://www.avast.com/index
  - ➢ AVG AntiVirus Free: http://free.avg.com/us-en/homepage
- ❑ If the device or a program notifies you that critical security updates or patches are available, promptly follow the instructions on the screen to download and install the updates.
- ❑ Set up password protection to log in to the device, wake the device, or unlock the screen; below are links to webpages with password how-to guides:
  - ➢ Apple OS: http://support.apple.com/kb/PH18668?viewlocale=en_US&locale=en_US
  - ➢ Windows: (a) http://windows.microsoft.com/en-us/windows/change-password-requirement-computer-wakes and (b) http://windows.microsoft.com/en-us/windows/windows-password-for-screensaver-password
  - ➢ Chrome OS: https://support.google.com/chromebook/answer/2587994?hl=en
  - ➢ iPhone/iPad: http://support.apple.com/en-us/ht4113
  - ➢ Android: https://support.google.com/playedition/answer/2819522?hl=en

- ❑ Log out of accounts and close browsers and programs whenever you are finished.
- ❑ Password-protect, lock, or otherwise secure all computers and devices when not in use.
- ❑ Immediately report lost or stolen devices to the administration.

Choosing Software and Web Applications

- ❑ Ask the administration whether your district or school has a policy about choosing software and web applications that may be used in the classroom or for other school purposes.
- ❑ Ask the administration if approval is necessary before downloading and using any software or web applications.
- ❑ Try all programs prior to inputting student data or using the program in the classroom.
- ❑ Consider whether the program requires you to enter student data or excessive information as a condition to use the program.
- ❑ Look for any advertisements displayed in the program, which may be a sign the program shares data with third parties.
- ❑ 

Analyze whether the program utilizes any security protocols, such as password protection or the web address includes the words "https" and a padlock symbol similar to this image:
- ❑ Avoid using any programs that appear to be suspicious.

Using Email

- ❑ Ask the administration whether your district or school has a policy about using email.
- ❑ Do not click on any links or download any attachments you receive from a suspicious source.
- ❑ Be cautious of emails containing the following:
    - ➢ Links in suspicious-looking messages
    - ➢ Threats that your account will be closed if you do not respond
    - ➢ Web addresses where names of well-known companies have been slightly altered
    - ➢ Requests for personal information
    - ➢ Unexpected attachments, especially those purporting to come from banks or financial institutions
    - ➢ Deals that sound too good to be true
    - ➢ Urgent emails demanding that you act immediately
    - ➢ Messages that list your email as the sender or from address

Accessing or Sharing Student Data

- ❑ Ask the administration whether your district or school has a policy about using or sharing student data.
- ❑ Only access the student data that you have permission to access.
- ❑ Only access student data for legitimate school or educational purposes.

- ❑ When accessing student data, only use computers or devices that have either been approved by the school or that contain security software and are password protected.
- ❑ Lock up hardcopy files and devices with access to student data.
- ❑ Do not share or disclose student data without authorization from an administrator, parent, or guardian.
- ❑ Do not share student data during public meetings or presentations; use fictitious records instead.
- ❑ Avoid sending student data via email unless specifically authorized.
- ❑ Immediately report any incidents to the administration where you believe student data may have been inappropriately accessed or shared.
- ❑

Bibliography and Resources

- Privacy Technical Assistance Center, Security Best Practices Toolkit: http://ptac.ed.gov/toolkit_data_security
- Colorado Department of Education, Data-Sharing & Confidentiality Agreement: http://www.cde.state.co.us/cdereval/cdeemployeedatasharingconfidentialityagreement

Microsoft Safety and Security Center: http://www.microsoft.com/security/default.aspx