CENTER FOR DEMOCRACY & TECHNOLOGY

A SERIES ON STUDENT PRIVACY & the HOMEWORK GAP

MANAGING DEVICES

Closing the Homework Gap While Protecting Student Privacy

A Quick Guide to Maintaining and Protecting School-Issued Devices

Closing the "homework gap" requires providing students with connected devices such as laptops and tablets. Flexible, privacy-forward device programs have become critical as coronavirus outbreaks, cyber attacks, and climate events have forced students and schools to move between in-person, hybrid, and remote learning. Device programs should protect student privacy throughout the devices' lifecycle, from distribution to return to retirement.

Prior to Distributing Devices

Inventory Devices and Document Privacy Measures such as Data Wiping

Schools may wish to track which devices are being used to provide students with technical support and ensure devices are returned. While tracking this data may be necessary, it may also pose risks to student privacy, especially where it includes sensitive information, such as which students require an accessibility device, like a sip-and-puff system or eye-tracking software, to be issued along with their device. This data requires robust data governance and security practices such as limiting access to and uses of the data. In addition, schools should document devices' conditions, when they have been wiped and updated, and the techniques used to wipe student data on the devices, as described below.

Wipe Previously Used Devices

When reissuing (or retiring) devices, schools should ensure that student data on the device is properly destroyed. This means following protocols for destroying any existing data left by the previous user, and ensuring that if that device is passed on to a new user, the former user no longer has access to the device or the information on it. These protocols should describe which destruction techniques should be used and what, if any, data should be archived and retained. At minimum, wiping procedures should address students' personal files, saved WiFi networks and locations, and user profiles. School protocols should also detail procedures for auditing the wiping and updating procedures to ensure they are adequate.

Update Devices, Including Security Patches

Schools should install the latest updates and security patches for the devices, including their applications and operating systems. Further, automatic or mandatory software updates can keep students safe by ensuring that they always have the latest security patches installed on their systems. Many users do not install system updates due to inconvenience or because they are simply unaware that they should do so. Setting up school-issued devices to update automatically avoids requiring users to manage this aspect of security on their own.

While Devices Are Lent Out

Provide Technical Support

Offering technical support is a key way to strengthen security, and one convenient way to offer technical support is by setting up school-issued devices to allow IT staff to access them remotely. However, for smaller or less technically mature schools, remote access can be a significant threat vector in its own right. Consequently, these schools may wish to use safer approaches to technical support, such as by-appointment office hours or a dedicated help line. Schools should also provide students and families methods for reporting lost devices, security lapses, or if a device was not properly wiped before receiving it. Where possible, schools should maintain the ability to remotely lock devices to help secure lost devices.

Communicate Reasons for and Changes in Policies

Schools should also explain device usage policies for students and families. Ensuring that students and families understand what harm the policies are intended to protect against can help garner buy-in to follow those policies more carefully. Students may be less likely to search for convenient workarounds to "inconveniences," like password protecting devices, if they understand that the workaround may undermine their safety and that of the rest of the school community. Changes to device policies — or to critical aspects of those devices such as major software updates — should be clearly communicated to students and families.

Upon Devices' Return

Engage Students and Families in the Return and Wiping Processes

Schools should engage students and families on procedures for returning and wiping devices, including whether students and families may benefit from retaining devices for longer periods (e.g., during in-person learning or the summer). Permitting families long-term access to devices may reduce administrative burdens, increase responsiveness to school closures or student's inability to attend in person (e.g., due to quarantine or suspension), and bolster students' digital skills. Prior to devices being returned, schools should provide clear notice of timelines for wiping devices and instruct families on how to retrieve and back up their students' data.

Retire Outdated Devices

Schools should plan to retire devices as they become obsolete — when they no longer receive security updates or are unable to run school programs efficiently — so as to not put the students using them at a disadvantage.

This two-pager is one of a series designed to give practitioners clear, actionable guidance on how to most responsibly use technology in support of students. Find out more at cdt.org/student-privacy.