

Personal Devices



UCLA Health IT does not take responsibility for personal devices. Laptops/desktops/mobile devices not owned or managed by UCLA Health IT are considered personal devices. Please be aware, as we are unable to account for all environments, operating systems, hardware/software, the information below is provided for informational purposes only and users must assume responsibility for personal devices. Additionally, we recommend following best practices by backing up your data before making any system changes to your device.

	Windows	Mac
Determine encryption status	Only one encryption tool is required. Check encryption for BitLocker	Check encryption for FileVault
Ensure minimum requirements	Approved Windows Versions for BitLocker: Minimum OS Requirement: Windows 10 build 22H2 (Professional, Enterprise, or Education edition) or newer. Locate Your Windows Version	FileVault Requirements: Minimum OS Requirement: macOS 13 (Ventura) or later Locate Your macOS Version
Before encrypting	Backing up your device prior to encrypting is suggested. Back up PC for Windows 10 or 11	Backing up your device prior to encrypting is suggested. Back up Mac
How to encrypt	For in-person assistance, please visit IT Connect . Do-It-Yourself Help: Instructions to turn on and set up BitLocker <i>(Instructions are for Windows 10—other Windows versions might differ slightly but instructions are overall the same.)</i>	For in-person assistance, please visit IT Connect . Do-It-Yourself Help: Instructions to turn on and set up FileVault