

Windows 11, Encryption, and You.

All new PC's that ship with Windows 11 come with a feature called either Device Encryption on Windows 11 Home, or Bitlocker on PC's with Windows 11 Pro. This feature enhances your computer's security by locking access to the drive where your Windows is installed. This feature is enabled by default on all versions of Windows 11 (Home or Pro) and is turned on the moment you set up a user account that is tied to a Microsoft account.

What Encryption means for you.

While Encryption keeps your data secure if your PC is lost or stolen, it can also cause issues with a lot of repairs. Due to the way the drive is protected certain repairs may not be possible such as things like removing a Windows Logon Password or even backing up files from a PC that wont boot properly. Pretty much any repair that would require accessing the drive without being able to log in to Windows may be a problem. If in doubt, ask your technician when checking your PC in for the repair.

How to bypass the Encryption.

There are not a whole lot of options to get around the encryption. The easiest option is to go into settings and disable it. While this does reduce security if the system is lost since the drive could be read by another machine, This does mean that the data is accessible and would be able to be backed up or transferred to a new machine if needed. The other option, which is only available in the Pro versions of Windows 11, is to save your Bitlocker Encryption key. This key will be automatically saved to the first Microsoft account set up on the PC but it is also possible to save it to a file or even write it down. With this key it is possible to unlock the drive to be able to access it for repairs or backing up files.