

1. Verify Windows edition

Note: A free upgrade to Windows 10 Education can be obtained through UMB's software sales page

- a. Click "Start", type "Winver" and click "Enter"
- b. Verify the version of Windows (right screenshot). Proceed to step 2 if Pro,Education or Enterprise. Upgrade Windows license if using Windows 10 Home

\equiv	All	Apps	Documents	Settings	Web	Ν	About Windows	×
ŵ	Best m	natch		•			Windows 10	
		winver Run comr	mand	3	\rightarrow		Microsoft Windows Version 1809 (OS Build 17763,503) © 2018 Microsoft Corporation. All rights reserved. The Windows 10 Enterprise operating system and its user interface are	
ŝ							This product is licensed under the <u>Microsoft Software License</u>	
_	́Р w	vinver	2				Terms to:	
	1						ок	

- 2. Initialize BitLocker
 - a. Click "Start", type "Manage Bitlocker" and click "Enter"
 - b. Click "Turn on Bitlocker" Windows will verify the system is ready for encryption. If the TPM is turned off, it may require to be enabled through the system BIOS. Please refer to your PC manufacturer (Most PC's now have this turned on by default)
 - c. Backup encryption key

🚽 👘 🕈 🙀 > Contr	rol Panel > System and Security > BitLocker Drive Encryption
Control Panel Home	BitLocker Drive Encryption
	Help protect your files and folders from unauthorized access by protecting your drives with BitLoc
	Operating system drive
	C: BitLocker off
	Turn on BitLocker

Note: This key is only needed in the event of hardware failure and will be necessary to pull any information off the hard drive in the event of system failure.

It is EXTREMELY important that this key is backed up in a safe location that you will have access to after graduation. <u>If your backup key is lost during after a hardware failure, data recovery will not be possible.</u>



School of Law IT recommends first using the Microsoft Account used to setup the laptop, and a 2nd means of storage (personal GDrive, OneDrive, DropBox). The key can also be printed or saved as a PDF to an **EXTERNAL** location. 2 or more methods of backup are highly recommended.

V

ow do you want to back up your recovery	/ key?
Some settings are managed by your system admini	strator.
A recovery key can be used to access your files and fold t's a good idea to have more than one and keep each ir	ers if you're having problems unlocking your PC. a a safe place other than your PC.
\rightarrow Save to your Microsoft account 1	
\rightarrow Save to a file	
\rightarrow Print the recovery key 3	
-	
low can I find my recovery key later?	

d. Follow the prompts to start encryption.

Note: Encryption can take a few minutes to a few hours. Keep device plugged in while encryption is completing in the background. You can return to normal tasks.

				* * C	
4	RitLocker Drive Encryption (C:)	÷	Real BitLocker Drive Encryption (C:)	÷	Ref BitLocker Drive Encryption (C:)
	Choose which encryption mode to use		Choose how much of your drive to encrypt		Are you ready to encrypt this drive?
	Windows 10 (Version 1511) introduces a new disk encryption mode (XTS-AES). This mode provides		If you're setting up BitLocker on a new drive or a new PC, you only need to encrypt the part of the drive		Encryption might take a while depending on the size of the drive.
	additional integrity support, but it is not compatible with older versions of windows.		that's currently being used. BitLocker encrypts new data automatically as you add it.		You can keep working while the drive is being encrypted, although your PC might run mo
	If this is a removable drive that you're going to use on older version of Windows, you should choose Compatible mode.		If you're enabling BitLocker on a PC or drive that's already in use, consider encrypting the entire drive. Encrypting the entire drive ensures that all data is protected—even data that you deleted but that might stil contain retrievable info.		Run BitLocker system check
	If this is a fixed drive or if this drive will only be used on devices running at least Windows 10 (Version 1511) or later, you should choose the new encryption mode		Encrypt used disk space only (faster and best for new PCs and drives)		The system check ensures that BitLocker can read the recovery and encryption keys co encrypting the drive.
	New encryption mode (best for fixed drives on this device)		O Encrypt entire drive (slower but best for PCs and drives already in use)		BitLocker will restart your computer before encrypting.
	O Compatible mode (best for drives that can be moved from this device)		La .		Note: This check might take a while, but is recommended to ensure that your selected works without requiring the recovery key.



Next

Cancel



Next Cancel



3. Verify key via Microsoft account (Optional)

a. If recovery is ever needed, it can be done through your Microsoft Account. Go to this link <u>https://account.microsoft.com/devices/recoverykey</u> and sign in. You'll be shown the device names, Key ID's and applicable Recovery Keys.

BitLocker recovery keys

Device Name	Key ID	Recovery Key	Drive	Key upload date	
				9/13/2018	Delete
				9/14/2018	Delete

Help with Microsoft account

- 4. Backup Key post-encryption (Optional) / Turning off BitLocker
 - a. You can always backup your key by going to the "Manage BitLocker" window (step 2a) and click **"Back Up your Recovery Key"**



b. Turning off BitLocker

Note: You are required to maintain an encrypted laptop while enrolled in the Clinical Law program. It is highly recommended you keep your laptop encrypted as it'll protect your data in the event of loss/theft. Turning off BitLocker can take quite some time. Please leave your device powered on during process.

