

CLPT IT BitLocker User Guide

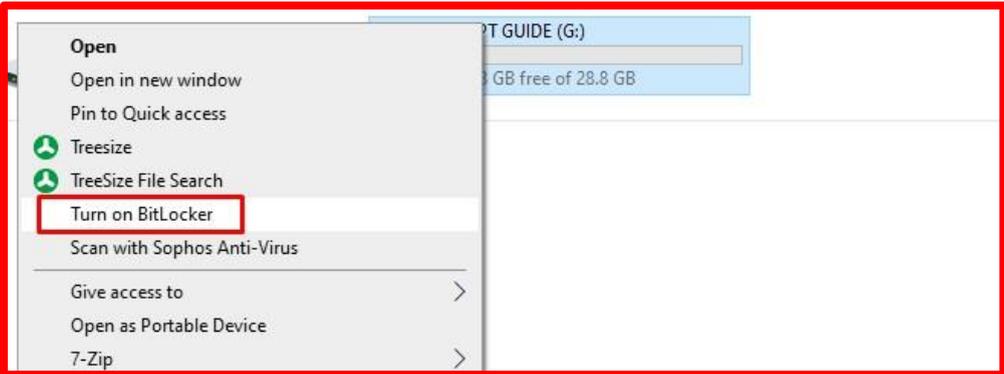
How to encrypt your USB removable
storage device

We would always recommend staff to utilise Office 365 One Drive or SharePoint in the first instance however if removable media is required and store ANY type of school related data it is compulsory that they are encrypted by BitLocker.

1. Locate your memory stick/hard drive in This PC (My Computer)



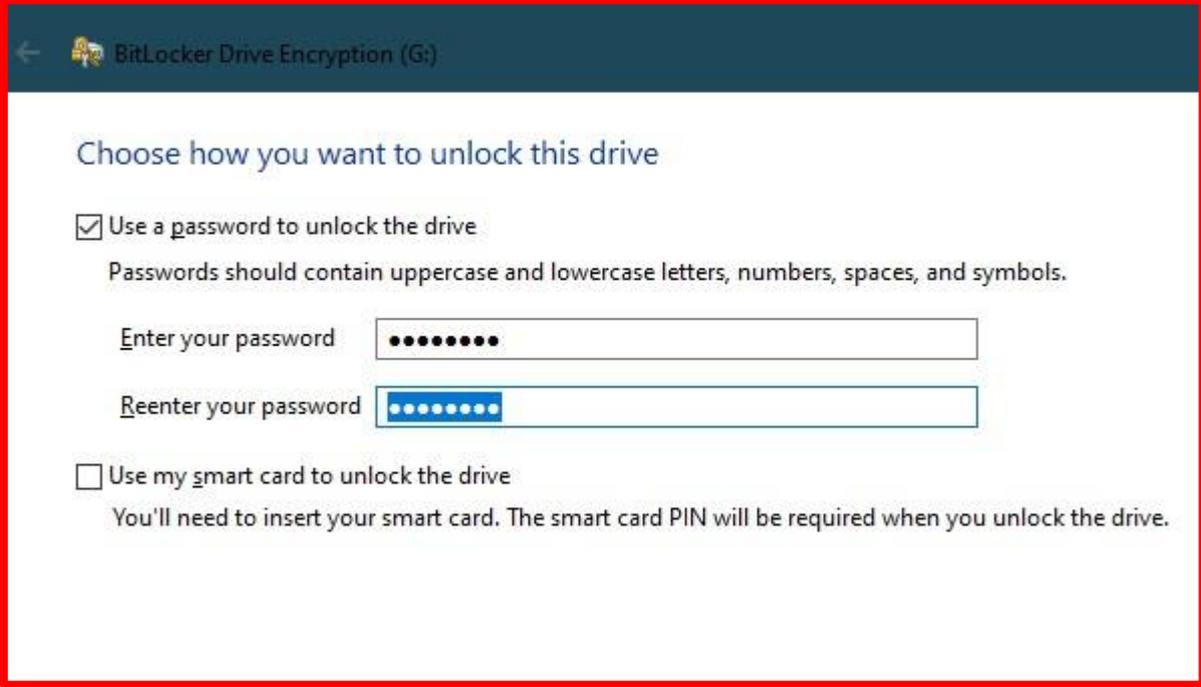
2. Once you have located your memory stick, right click and select Turn on BitLocker...



3. The BitLocker wizard will now prepare and initialise your drive.



- You now need to select “Use a password to unlock the drive” – enter a secure password and please make sure you store the password somewhere at home or in your phone, if you lose this password we can not get work back off the memory stick for you.



← BitLocker Drive Encryption (G:)

Choose how you want to unlock this drive

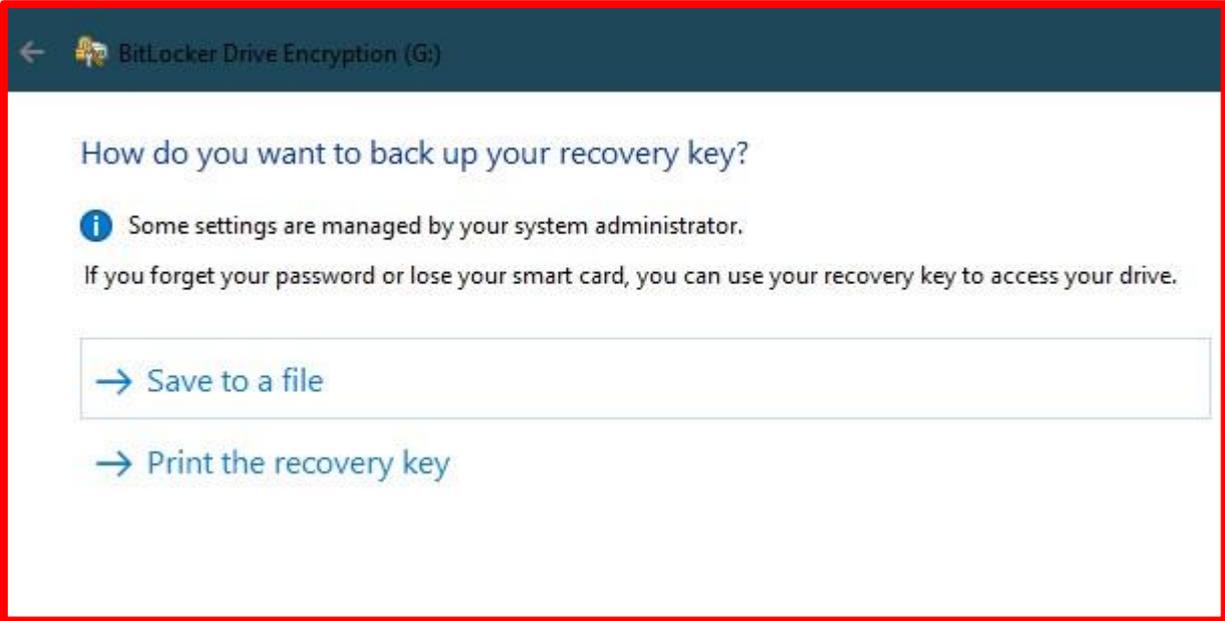
Use a password to unlock the drive
Passwords should contain uppercase and lowercase letters, numbers, spaces, and symbols.

Enter your password

Reenter your password

Use my smart card to unlock the drive
You'll need to insert your smart card. The smart card PIN will be required when you unlock the drive.

- Backup your recovery key. **Please note: you can not save your recovery key on the USB drive you are encrypting.** Please save it somewhere like your home pc/laptop or your school OneDrive account, alternatively print the key off and store it at home.



← BitLocker Drive Encryption (G:)

How do you want to back up your recovery key?

i Some settings are managed by your system administrator.
If you forget your password or lose your smart card, you can use your recovery key to access your drive.

→ Save to a file

→ Print the recovery key

6. Once you have saved your recovery key somewhere, simply press Next on the BitLocker wizard.
7. Now you need to select “Encrypt used disk space only” – it is always recommended to BitLocker a brand-new USB drive or formatted USB disk, if you have a lot of work on your personal device this **may take a while**. Please **do not** remove your USB drive from the computer at this point of encrypting. This will corrupt the device and lose everything, the wizard may take between 5-30 minutes depending on how much data you have.

Choose how much of your drive to encrypt

If you're setting up BitLocker on a new drive or a new PC, you only need to encrypt the part of the drive that's currently being used. BitLocker encrypts new data automatically as you add it.

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 still contain retrievable info.

- Encrypt used disk space only (faster and best for new PCs and drives)
- Encrypt entire drive (slower but best for PCs and drives already in use)

8. Because you are most likely going to use this USB device around the school and not on the same PC – please leave your USB drive in “Compatible mode” as this will work on multiple devices.

Choose which encryption mode to use

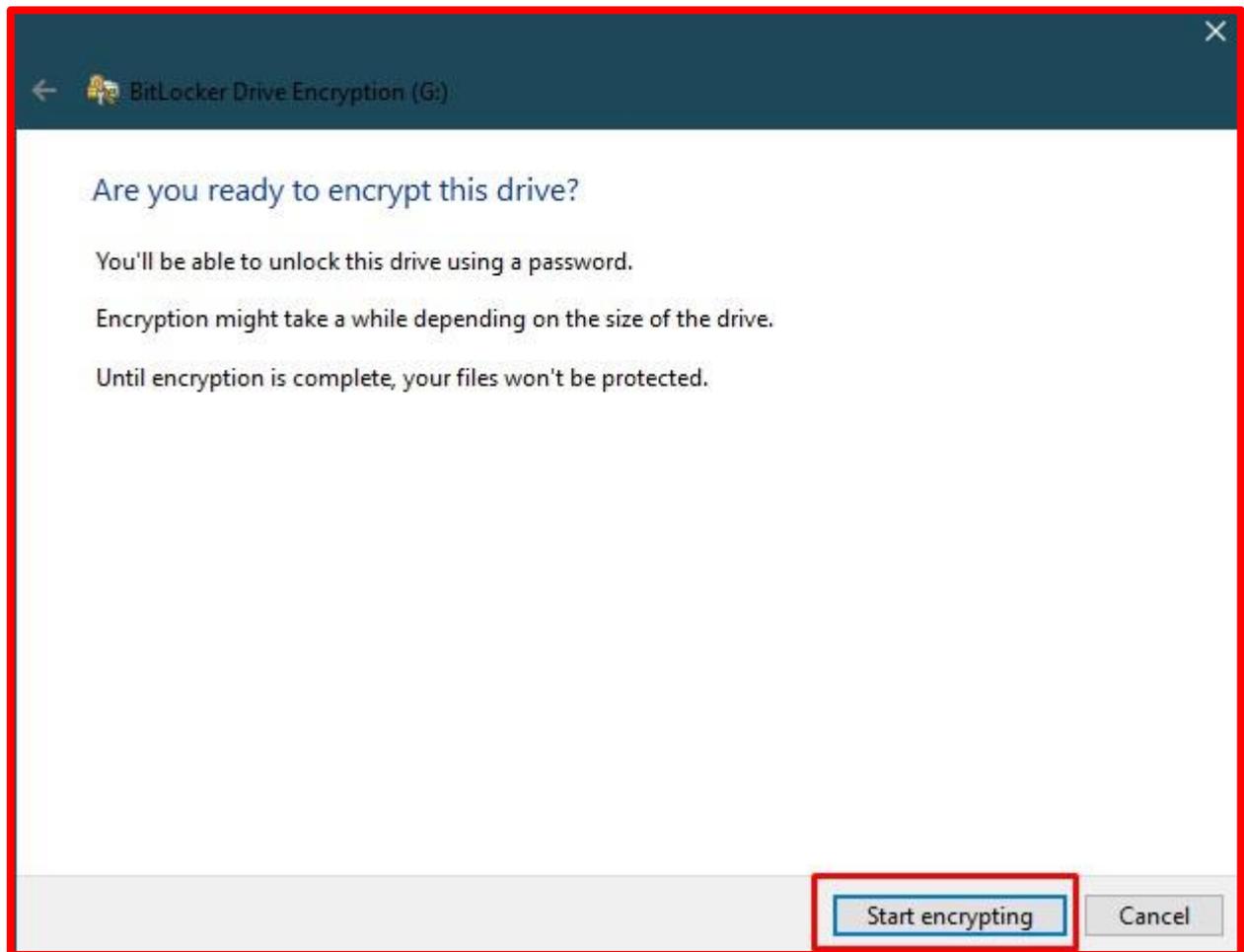
Windows 10 (Version 1511) introduces a new disk encryption mode (XTS-AES). This mode provides additional integrity support, but it is not compatible with older versions of Windows.

If this is a removable drive that you're going to use on older version of Windows, you should choose Compatible mode.

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

- New encryption mode (best for fixed drives on this device)
- Compatible mode (best for drives that can be moved from this device)

9. You are now ready to encrypt the USB drive. Select **Start encrypting** to begin the encryption.



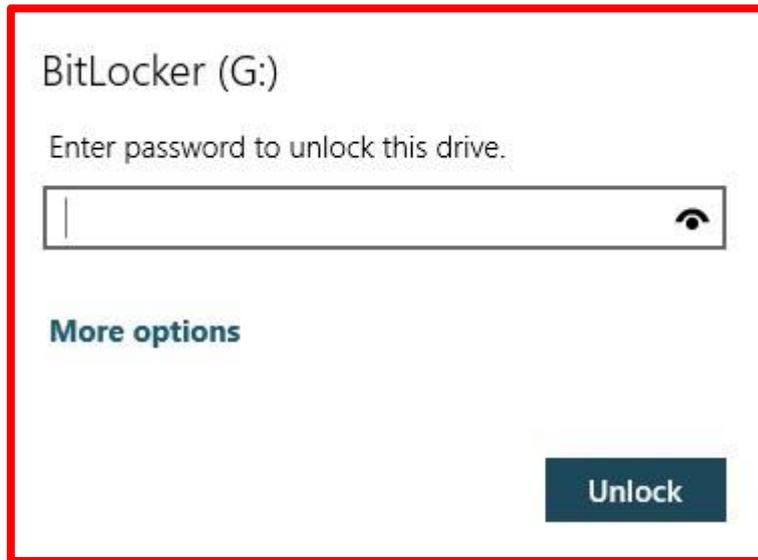
10. You will now see a pop up box appear saying "Encrypting" please do not remove your device at this point as the drive could be damaged or corrupted.



11. The BitLocker Drive Encryption tool will close when completed and disconnect your USB drive from the computer automatically, please re-connect your drive to the computer and this time it will prompt you to enter the password.



Click this message to unlock the password box, alternatively, go to My Computer and double click your USB drive and the password box will prompt you to enter your BitLocker password in.



If you have any further questions, please feel free to log a ticket on our helpdesk (helpdesk@clpt.co.uk) – or call IT Support on 01902 556493.

