Bitlocker Encryption

Accessing Bitlocker Key or Disabling Encryption

What is Bitlocker Encryption? Bitlocker is a security measure used by Windows devices to protect your data. If your computer was lost or stolen, Bitlocker encryption protects your data from being accessed by other parties.

If your BYOD laptop has Bitlocker encryption enabled and you want to make changes to the device in future (like reformatting or updating) it may require a **bitlocker key** to access the disk drive.

PLEASE READ: You may not be aware that your device has been bitlocker encrypted but this happens automatically when you sign into Windows with a Microsoft account. You must check this before you leave the school. Churchlands is not responsible for the recovery of bitlocker encryption keys once you have left the School.

The following instructions explain how to see if your device is Bitlocker Encrypted and how to **retrieve the key** or **turn off encryption** if necessary.

Check if your device is Bitlocker Encrypted

1. Type **Manage Bitlocker** into Windows search box. Click on Manage Bitlocker option
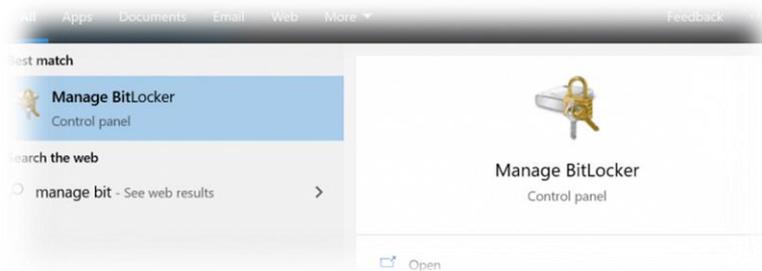
2. On the following screen it will tell you if Bitlocker is turned on under operating system drive

Bitlocker Encryption

If Bitlocker is turned on please follow the instructions below.

To retrieve your Bitlocker key

1. Select the Back up your recovery key option (put in the Administrator password for device if this is requested)
2. Put in an external device (USB or hard drive)
3. Select the Save to File option and save the key to the external device
4. Alternatively you can select to print the key and keep it on a print out

To turn Bitlocker off

1. Plug your device into a power source
2. Select the Turn off Bitlocker Encrytion option option (put in the Administrator password for device if this is requested)
3. Select the Turn Bitlocker off option
4. Leave device plugged into power while it decrypts the drive

The Decryption process can take anywhere from 20 minutes to 3 hours to complete.