Inspiring success

Teesside University

June 2017

ITACS Information Assurance
USB Memory Stick Guidance

Note: Information held on a portable USB device must always be a copy of an original held on a University computer system. This is necessary to ensure that this information remains accessible to authorised users even if the portable device is lost, damaged or stolen.

If you suspect that confidential information in your care has been lost, stolen, tampered with or disclosed without authorisation, report the incident immediately to the Information Assurance Team on 01642 342220 or email ithelp@tees.ac.uk

Prompt reporting of problems will enable staff to take effective action to mitigate any consequences.

All users of confidential University information have a responsibility to take appropriate measures to minimise the risk of this data falling into the hands of people who do not have the right to see it. The University takes its responsibilities for information security very seriously. Failure to comply with the University Security policy is a disciplinary offence which may include action up to and including dismissal. Serious breaches of the policy, whether intentional or nonintentional, and which place the University at serious financial, commercial or reputational risk or actual loss may be considered as gross misconduct offences, for which summary dismissal may be an outcome. You can find the latest relevant version of the University policies here –

Information Security Policy	http://url.tees.ac.uk/isp
Acceptable use Policy	http://url.tees.ac.uk/aup

Before copying University data onto any removable device, please consult the University Information Security Policy.

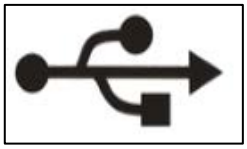
itacs

Department of IT and Communications Services

How to Encrypt a USB Memory Stick (Windows 7 & 10)

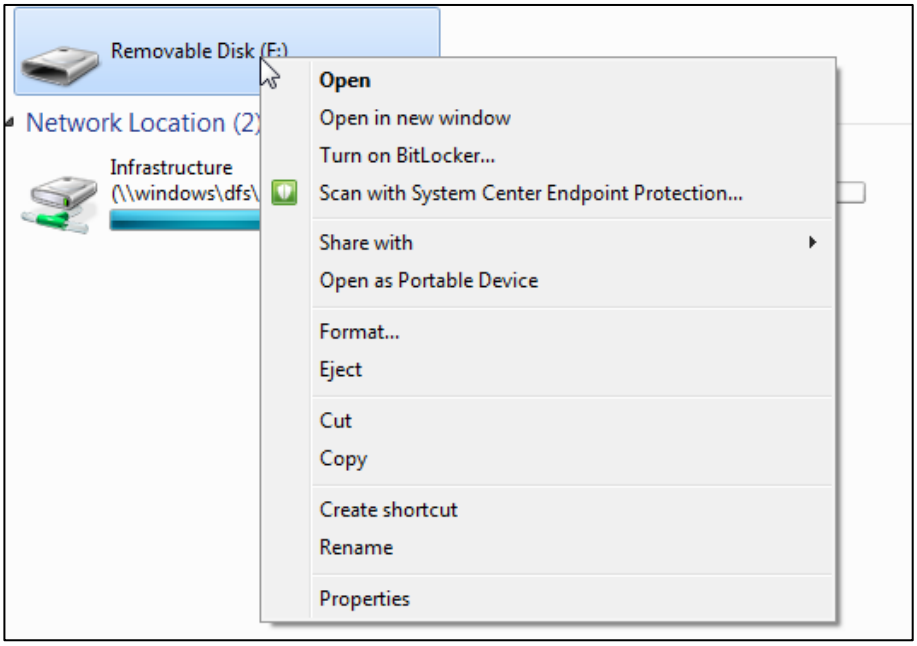
(Please note that the interface looks slightly different in Windows 10)

- Insert your USB stick into the computer's USB port. The USB port will be marked with the following symbol –

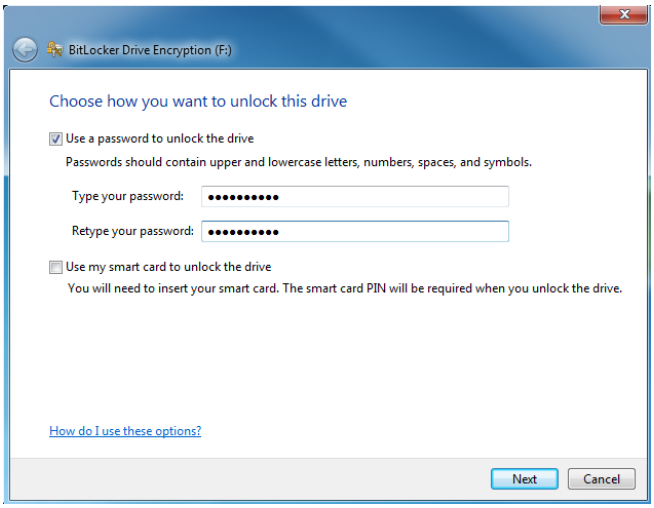


- Open Windows Explorer, and look for your USB stick. It should appear as 'Removable Disk' or it may have been given another name.

- Right click on the device in Windows Explorer, and select "Turn on Bitlocker"

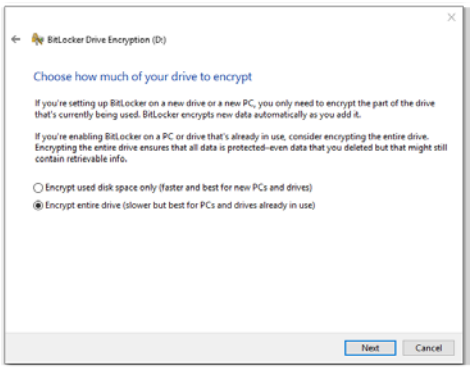


- Select the Tick box titled 'Use a password to unlock the drive'
  Pick a strong password, and remember it. Ensure that you correctly re-enter the password



- Save the recovery key to your U Drive, or somewhere safe. Don't keep it in the same place as your USB key, as it can be used to access the files on the drive. The recovery key can be used to unlock the key if you forget your password.

- On Windows 10 only, you will be asked "Choose how much of your drive to encrypt" Choose "Encrypt entire drive' This means that older PC's running Windows 7 will be able to access the drive. It does mean the initial encryption will take longer to perform.



- The device will begin to encrypt. Depending on the size of the drive, this may take some time. You will only have to go through this process once, when you initially encrypt the device.

Using the Device

- Insert the USB device into the computer. Before you can use it, you must unlock it with the password that you created.

- Simply enter ther password and the device will appear in Windows Explorer ready to use.

- You can find the encrypted USB in windows explorer. It will appear as follows -