ENCRYPTING USB REMOVABLE MEDIA

Telford Langley School ICT Services

Version 1.0

December 2021

WHAT YOU NEED TO NOTE

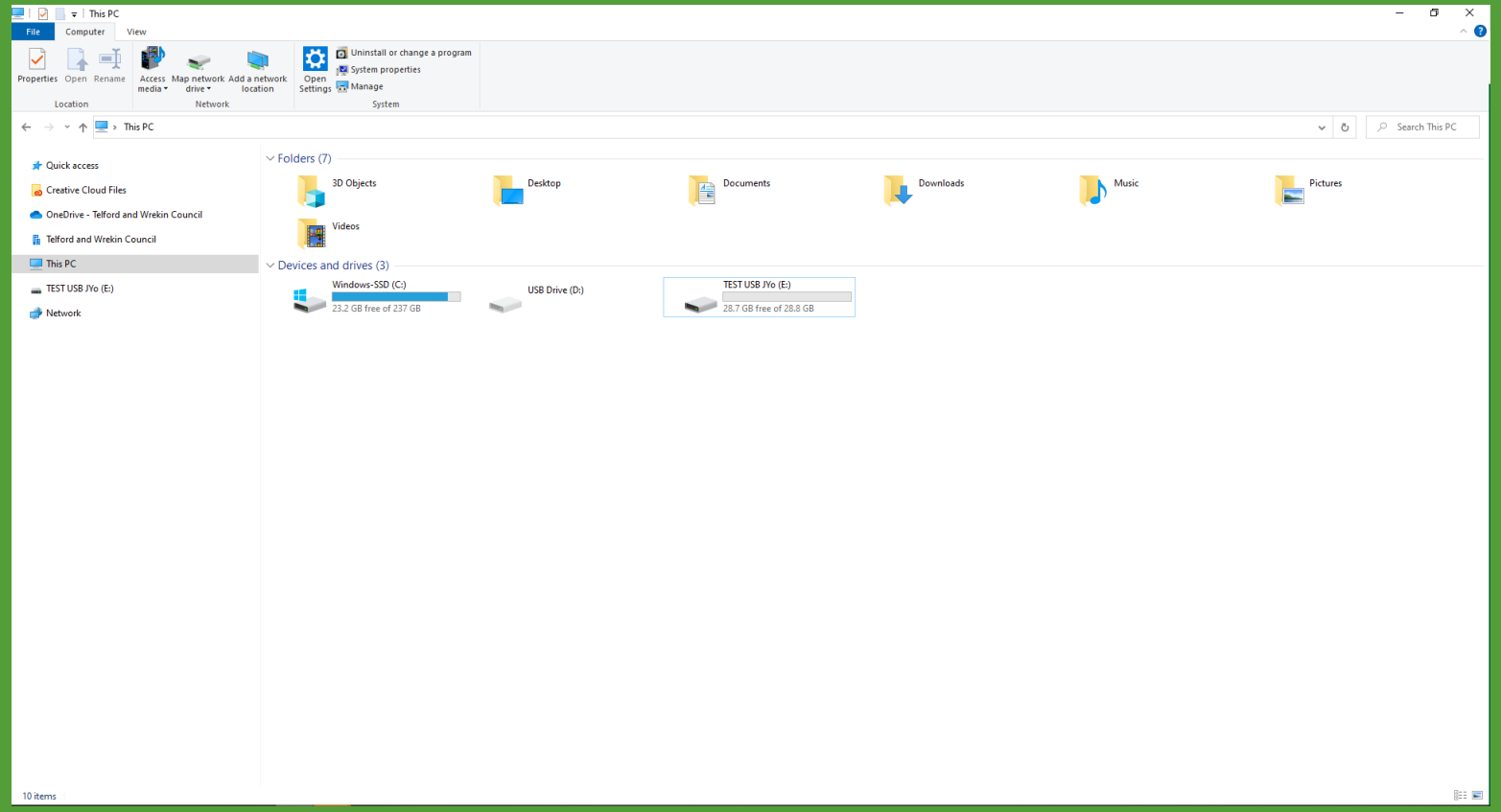
- If you use removable media sources such as USB hard drives and memory sticks they must be encrypted to reduce the risks associated.
- It is best practice to store school related data and documents on Office 365 applications such as OneDrive and SharePoint.
- If staff do wish to use removable media devices in school they **MUST** be encrypted, this document will show you step by step on how to do this or ICT Services will be happy to do this on your behalf.
- Staff should familiarise themselves with associated CAT policies and ensure any data sharing and storage is in-line with the trust's data protection policy and information security policy at all times.
  - CAT Information Security Policy
  - CAT Data Protection Policy

HOW TO CORRECTLY ENCRYPT YOUR REMOVABLE MEDIA

Via BitLocker

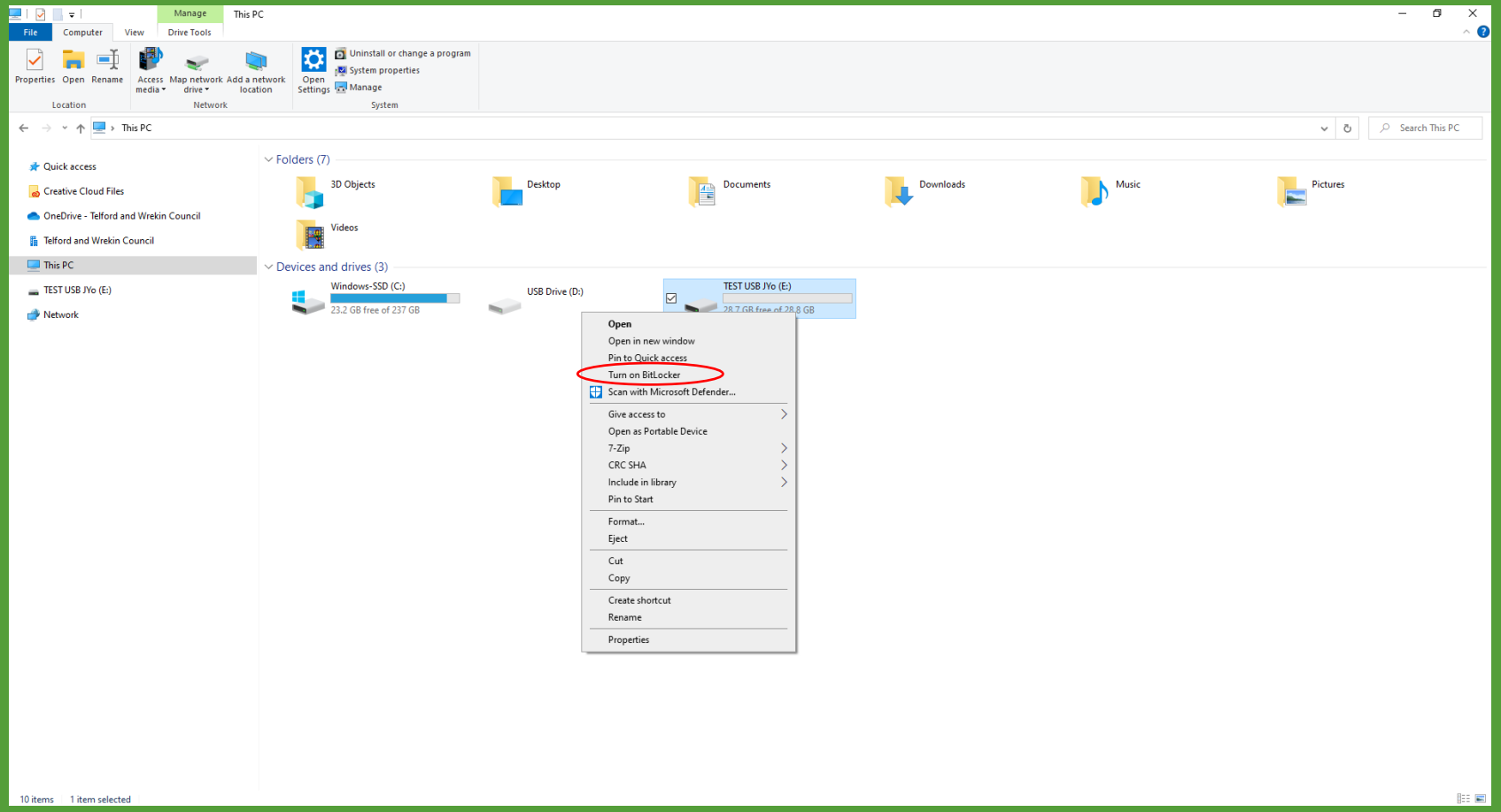
STEP 1

On a school issued device connect your removable media device and open up file explorer.



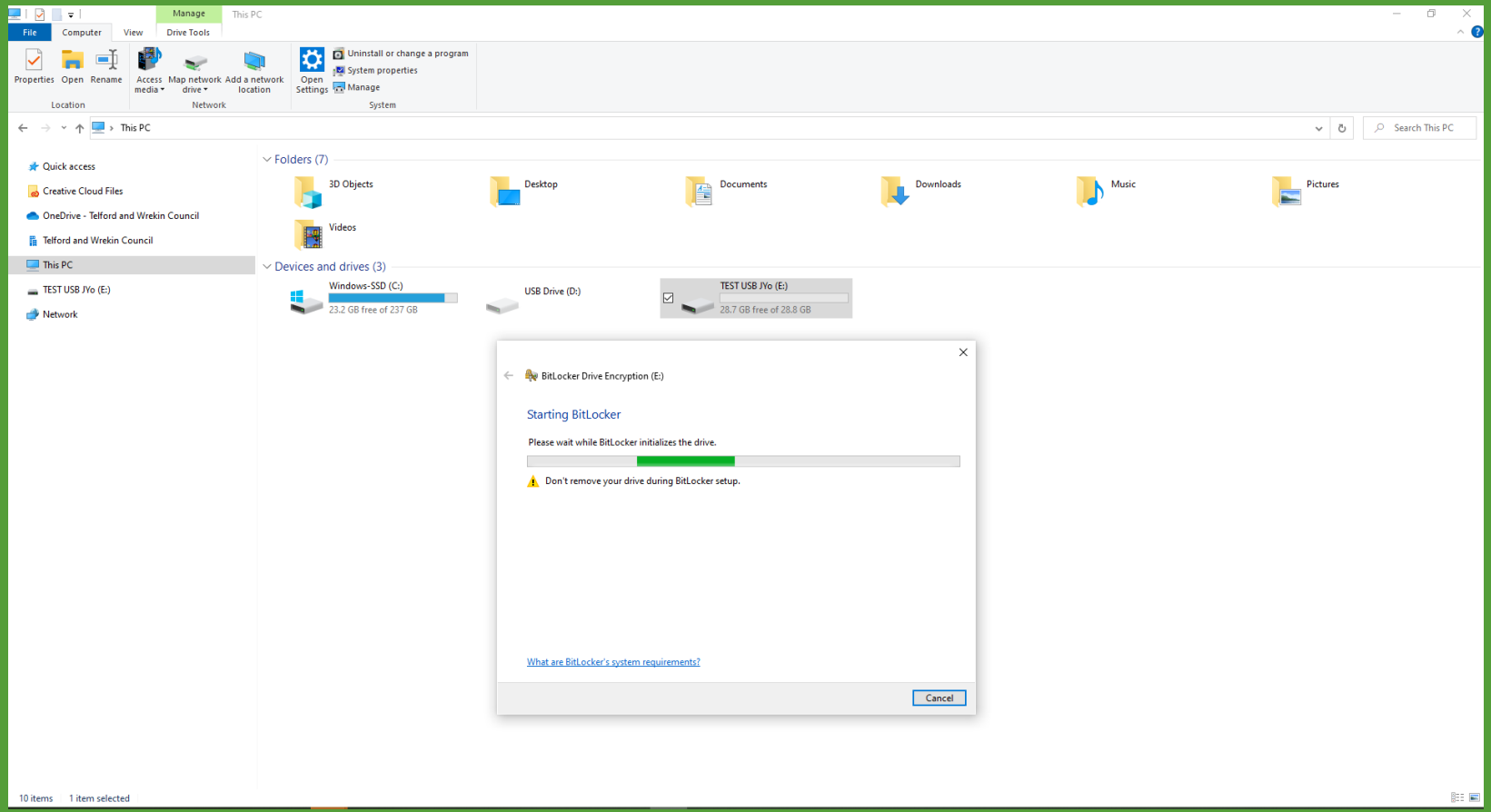
STEP 2

Right click your removable media device and click ‘Turn on Bitlocker’



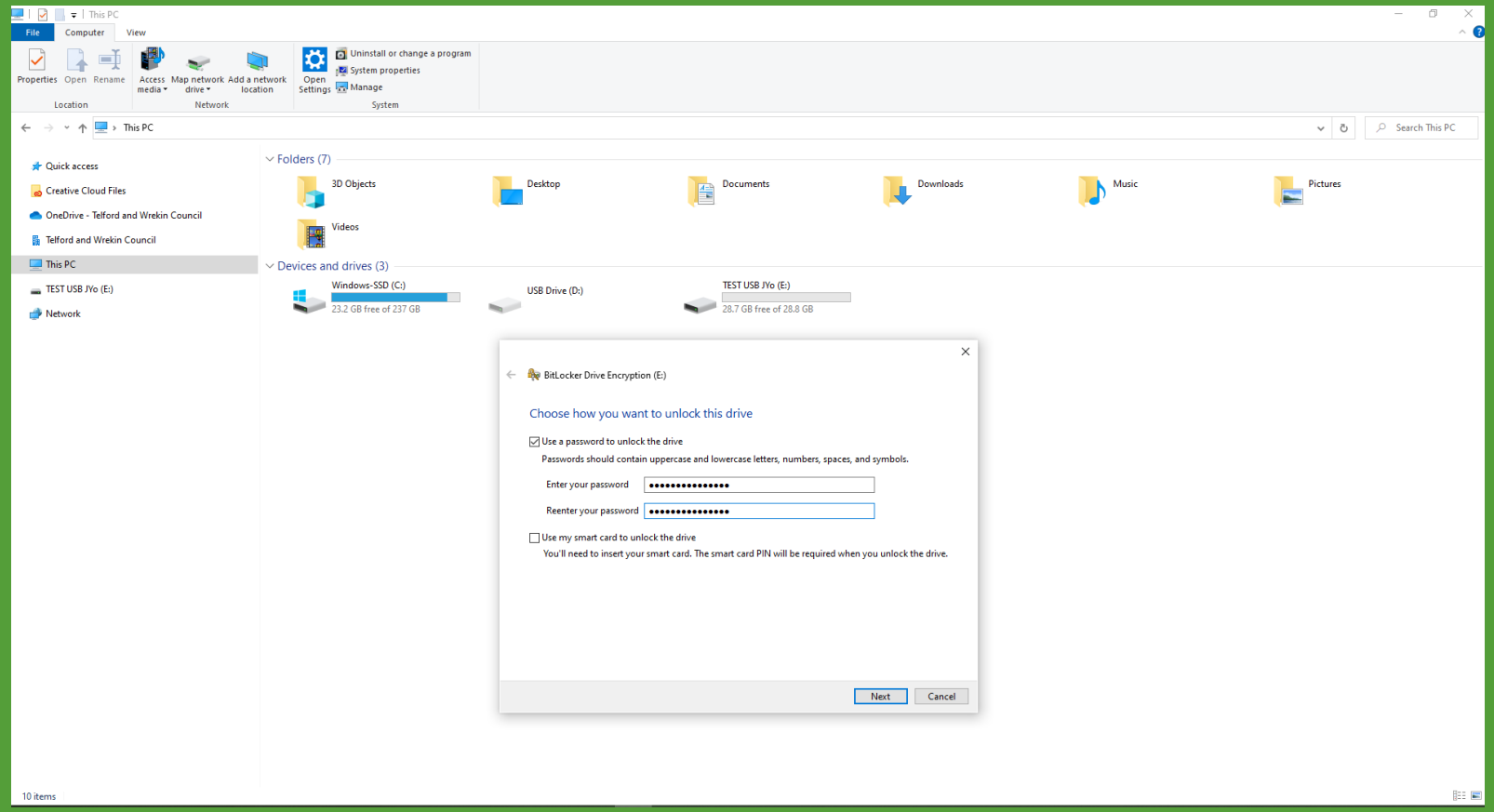
STEP 3

Your device will then start an initial scan and check of the device.



STEP 4

You will then be prompted to set a password. This should be in-line with Microsoft's best practise password guidance on the slide below. This should differ to your laptop password.



MICROSOFT'S PASSWORD GUIDANCE

https://www.microsoft.com/en-us/research/wp-content/uploads/2016/06/Microsoft_Password_Guidance-1.pdf

STEP 5

Whilst securing your removable media, it is important you don't want to end up locking yourself out of your media device.

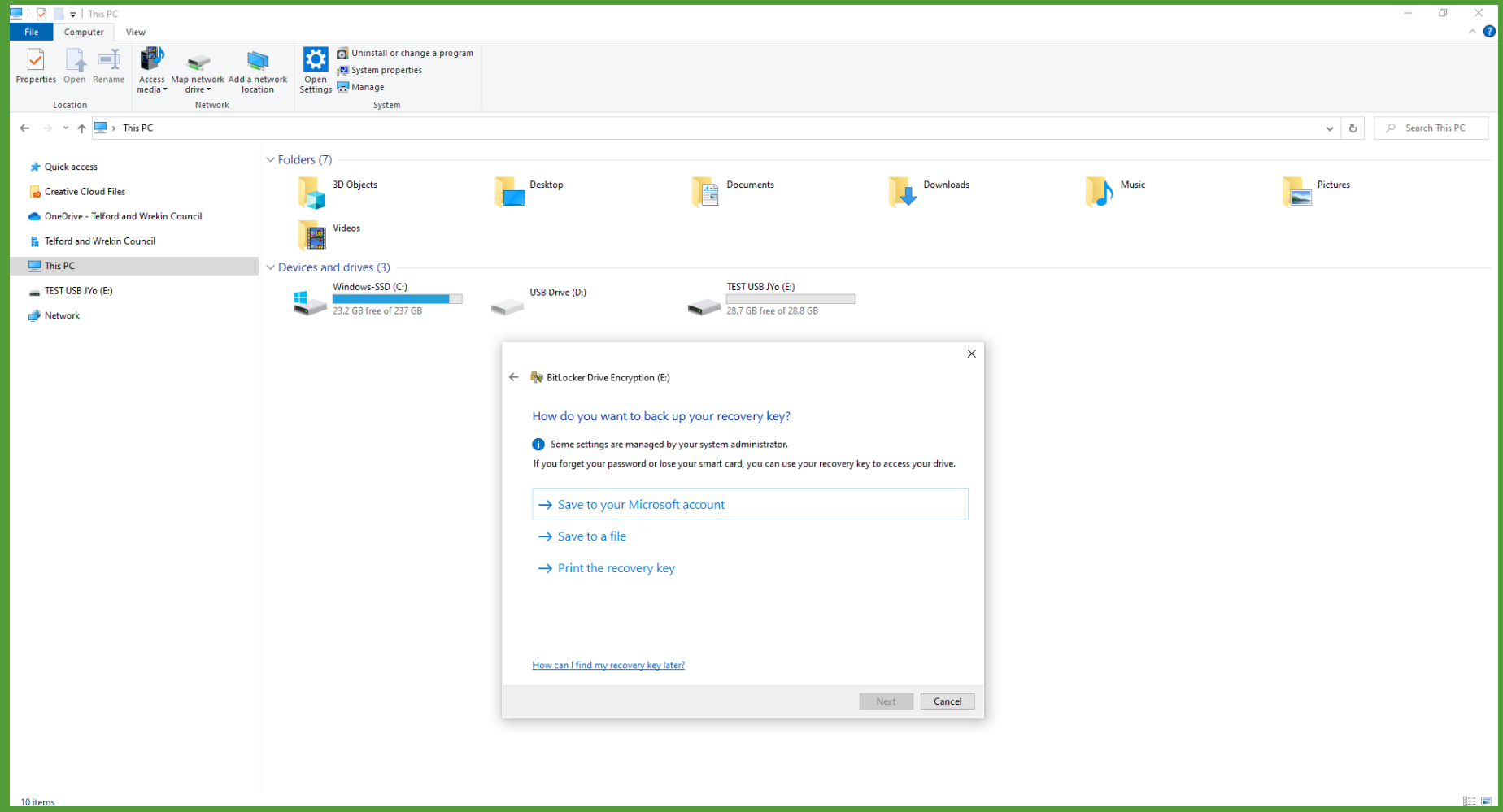
When you set up your password Bitlocker generates a recovery key so if you did forget your password you can assess your device.

You need to save this key to your Microsoft account and/ or print this key and keep the paperwork somewhere safe and private.

These are options provided when you set up the encryption.

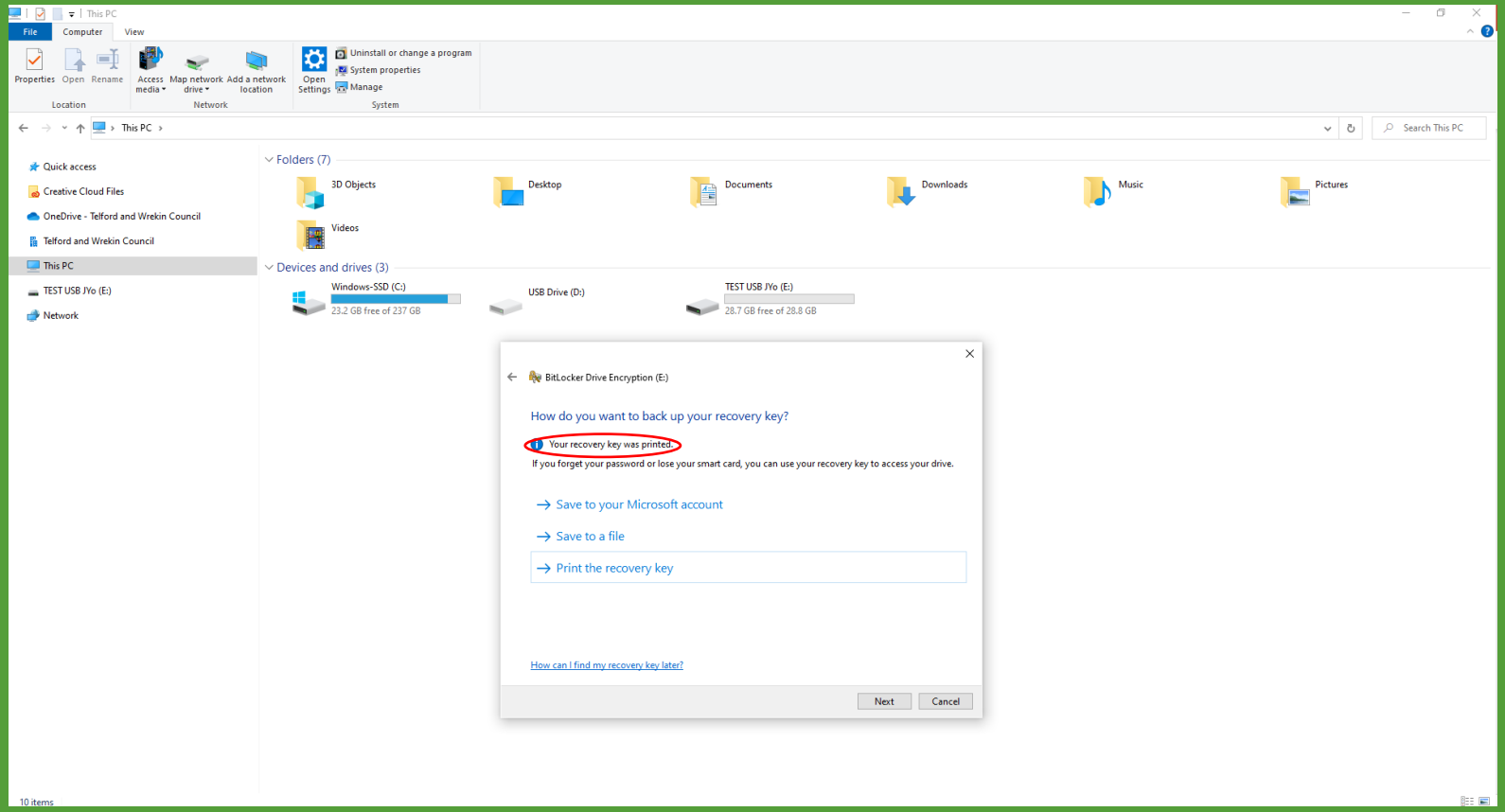
The slide below demonstrates the options available during encryption set up.

STEP 5


This PC
File
Computer
View
Properties
Open
Rename
Location
Access media
Map network drive
Add a network location
Network
Open Settings
Uninstall or change a program
System properties
Manage
System
This PC
Search This PC
Quick access
Creative Cloud Files
OneDrive - Telford and Wrekin Council
Telford and Wrekin Council
This PC
TEST USB JYo (E:)
Network
Folders (7)
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Devices and drives (3)
Windows-SSD (C:)
23.2 GB free of 237 GB
USB Drive (D:)
TEST USB JYo (E:)
28.7 GB free of 28.8 GB
BitLocker Drive Encryption (E:)
How do you want to back up your recovery key?
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 your Microsoft account
Save to a file
Print the recovery key
How can I find my recovery key later?
Next
Cancel
10 items

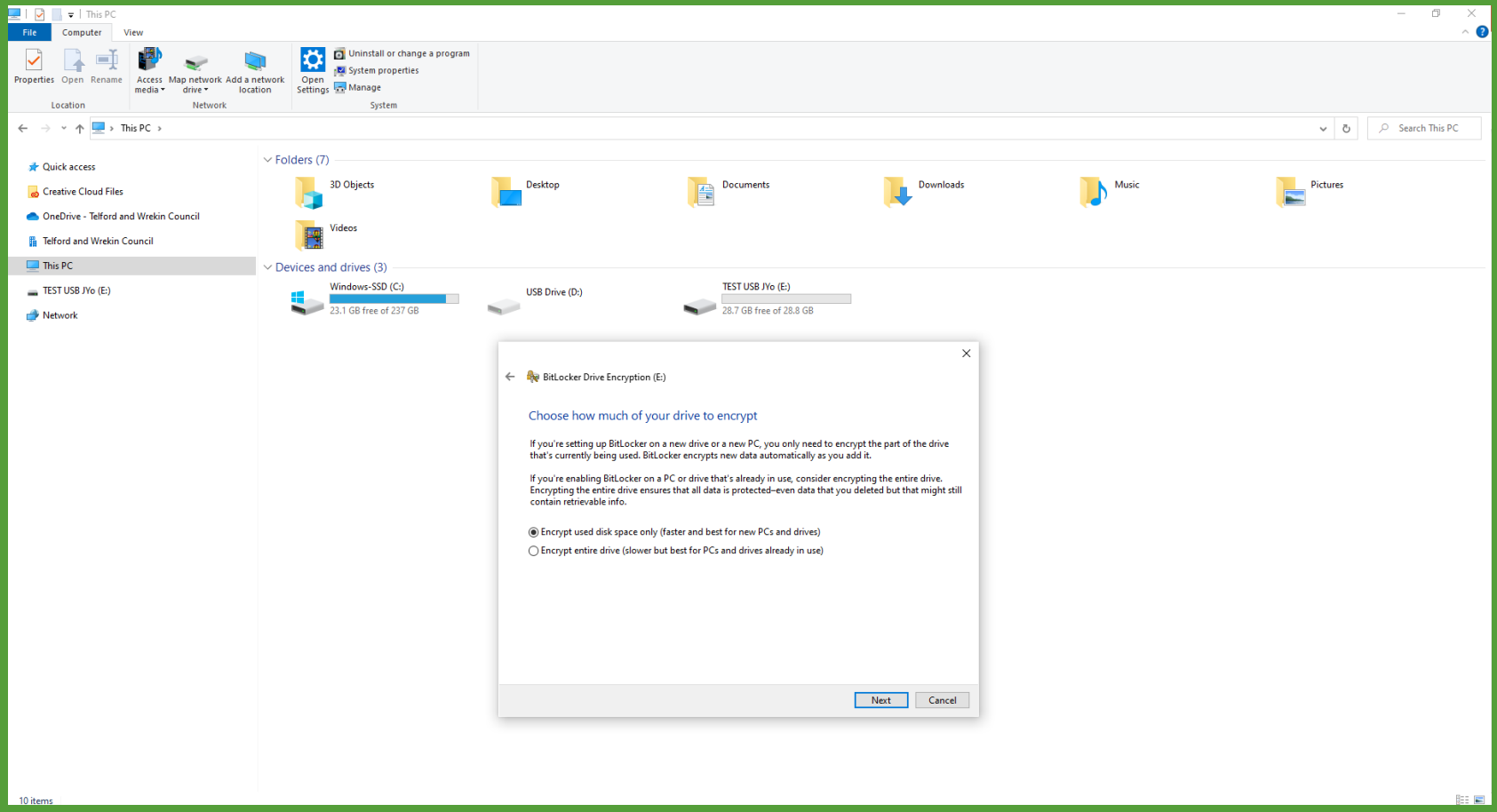
STEP 6

Once you have saved and/ or printed your recovery key you'll be able to continue.



STEP 7

Setting your encryption type.

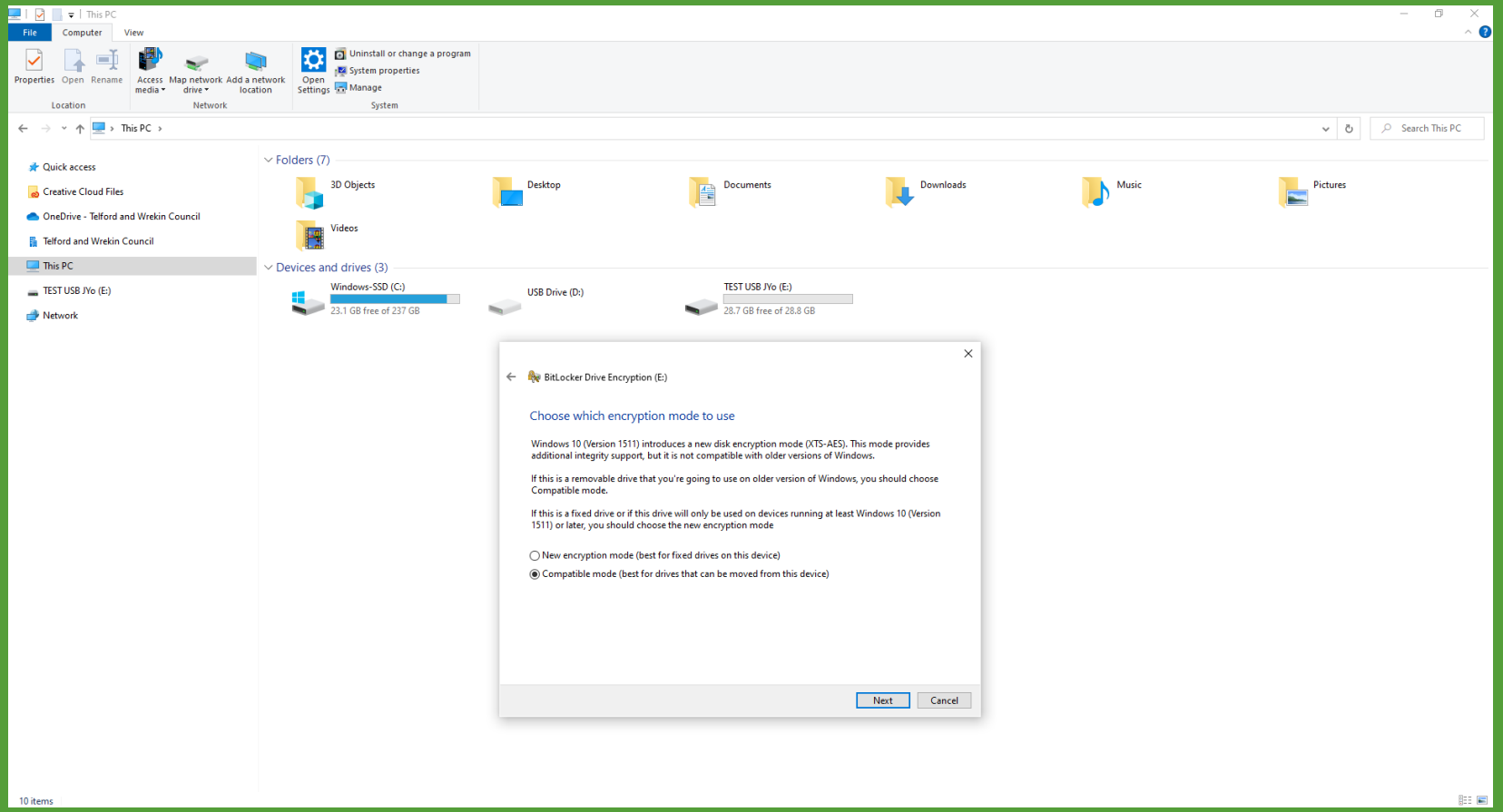


Already in use USB – option 1

New USB – option 2

STEP 8

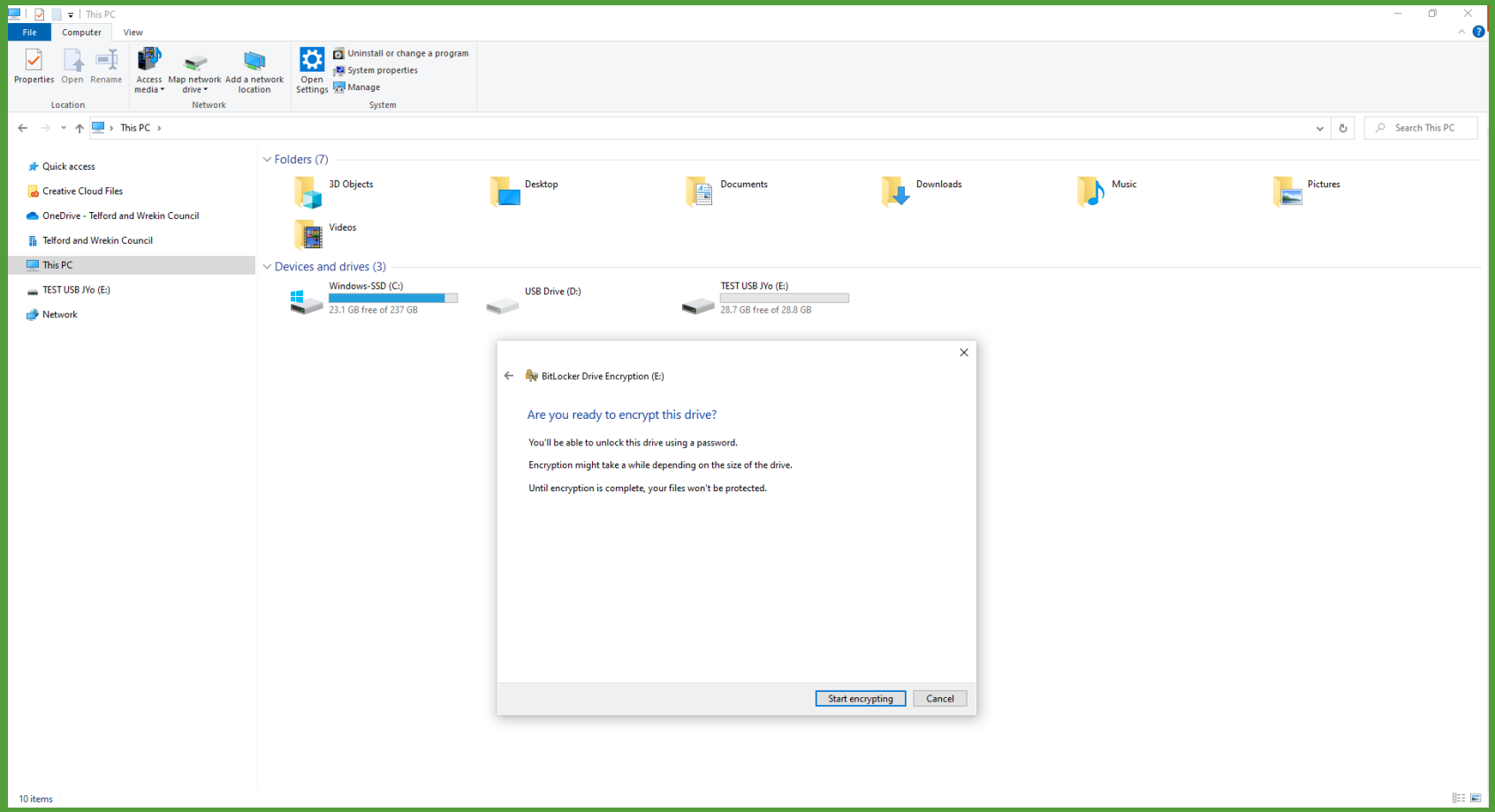
Setting your encryption mode.



If you use a range of devices of different ages we would recommend compatible mode.

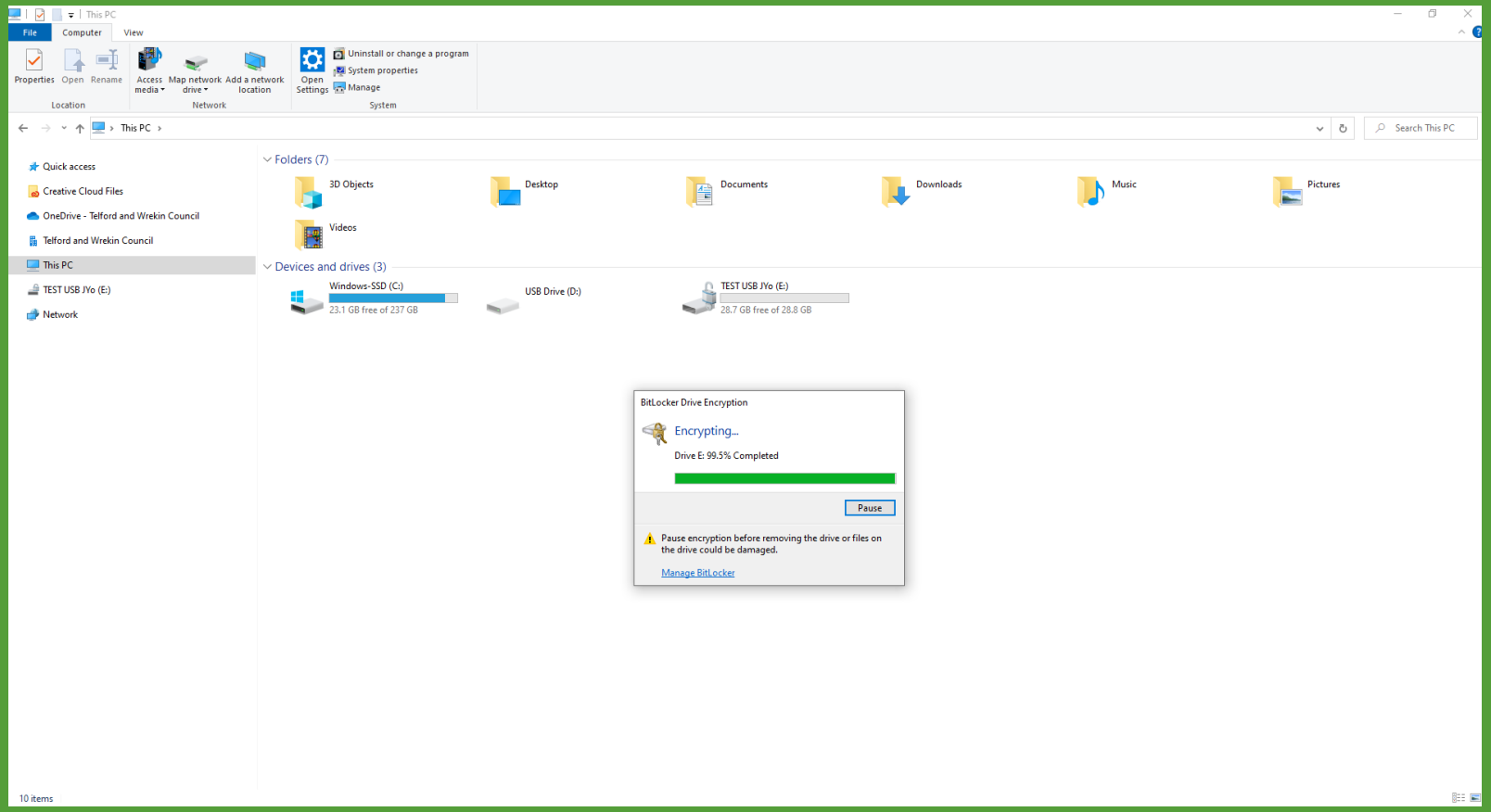
STEP 9

You’re now ready to encrypt your device!



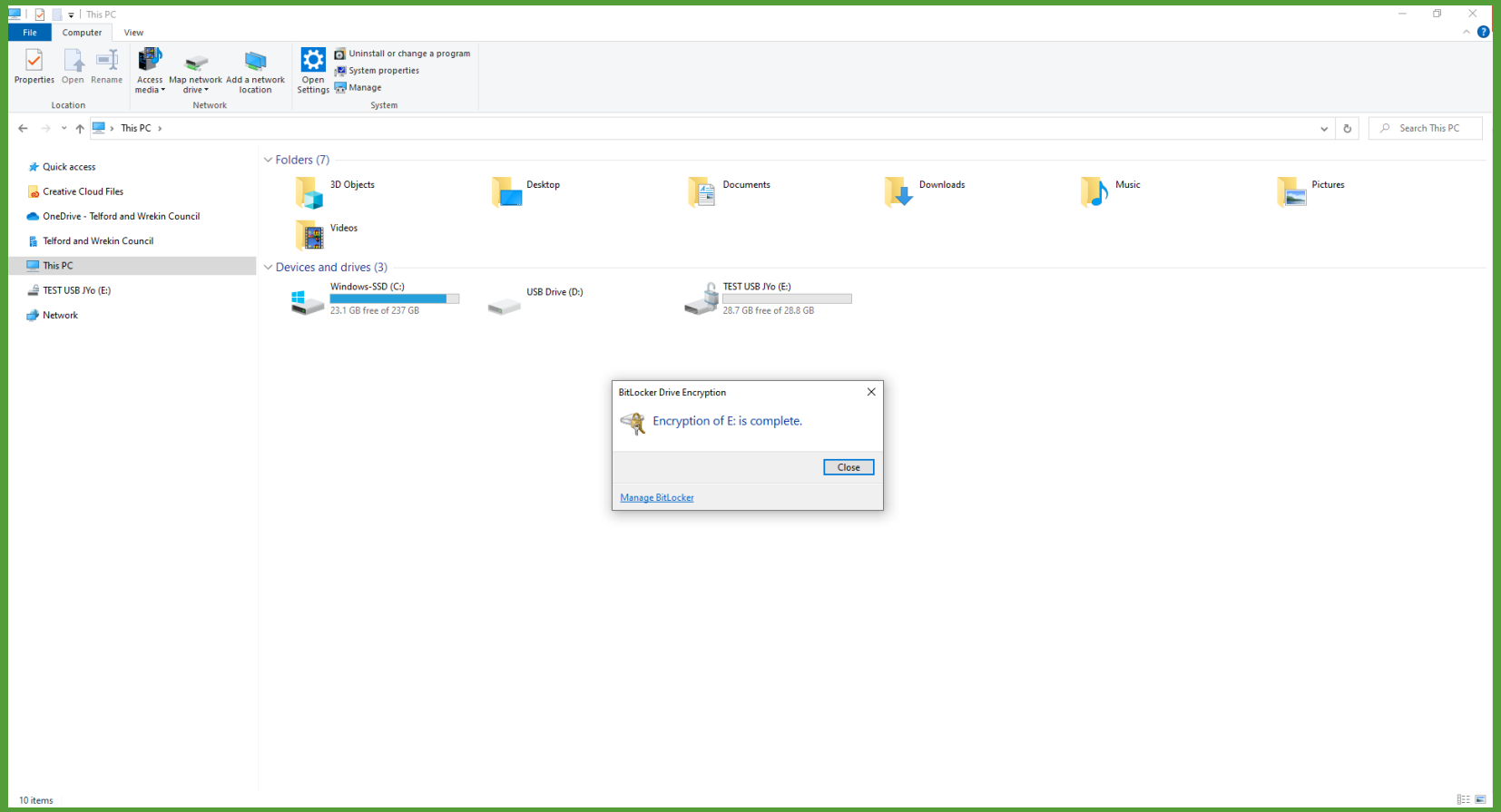
STEP 10

Depending on the amount of data on the device the encryption time may vary.



STEP 11

Once complete you'll get a pop-up box confirmation.

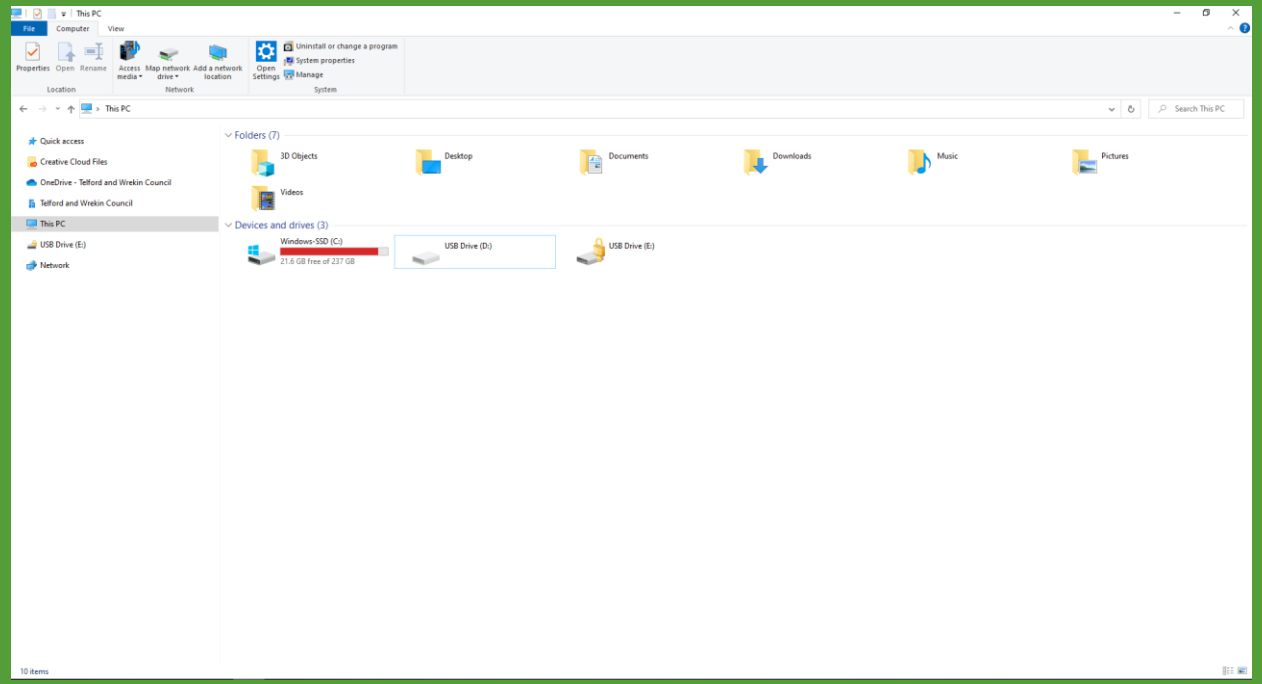


USING YOUR DEVICE MOVING FORWARD

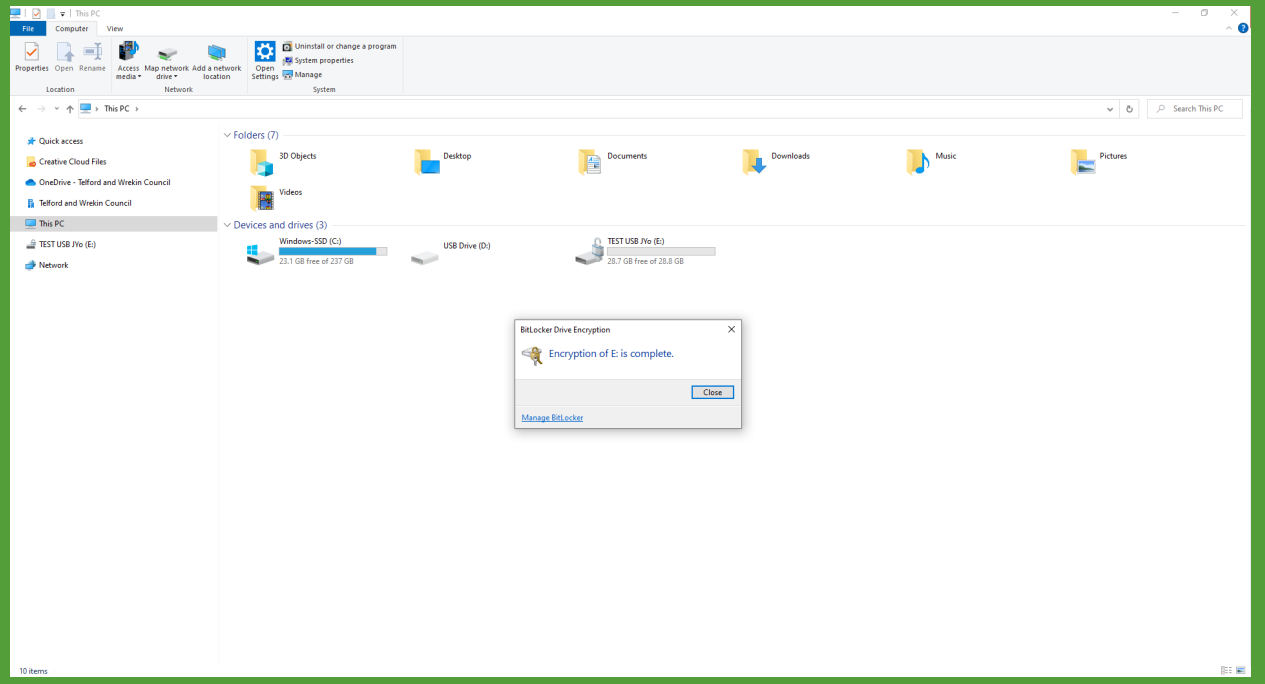
The lock status of the device will be indicated with in File Explorer and you'll be prompted for your password for the device every time you plug it in.

To unlock simply double click the removable media device in File Explorer.

Connected and awaiting unlock



Unlocked and ready to use



CONCLUSION

- School managed services such as One Drive and Office 365 for storing data is a highly recommended preference and should be used in most cases.
- Any removable media including school related data **MUST** be encrypted.
- Staff should familiarise themselves with the Community Academy Trust's policies including; information security and data protection, in-particular the use of removable media.
- Any problems, questions or queries should be logged with ICT Services via the support desk – http://icts.telfordlangleyschool.co.uk

ISSUES, QUESTIONS OR QUERIES

http://icts.telfordlangleyschool.co.uk