
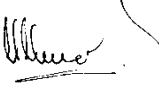


SOP - 21

Device & File Encryption (mobile and storage devices)

VERSION NUMBER	1.2	DATE OF VERSION (dd/mm/yyyy)	1	3	/	0	1	/	2	0	1	7
-----------------------	-----	------------------------------	---	---	---	---	---	---	---	---	---	---

WRITTEN/REVIEWED BY	Print Name	Angela Attwood										
	Position	Research Fellow										
	Signature											
	Date (dd/mm/yyyy)	0	3	/	0	2		2	0	1	6	

APPROVED BY	Print Name	Marcus Munafò										
	Position	Professor of Biological Psychology										
	Signature											
	Date (dd/mm/yyyy)	0	3	/	0	2	/	2	0	1	6	

DATE OF NEXT SCHEDULED REVIEW (dd/mm/yyyy)	1	3	/	0	2	/	2	0	2	1
---	---	---	---	---	---	---	---	---	---	---

REVIEWED BY	Print Name	Maddy Dyer											
	Position	Research Associate											
	Signature												
	Date (dd/mm/yyyy)	1	3	/	0	2	/	2	0	2	0		
	Outcome of review:												

Table of Contents	Page
1. PURPOSE	2
2. REFERENCE	2
3. PROCEDURE	2
3.1 Enabling encryption on your laptop or memory stick	
4. TROUBLE SHOOTING	2

Definitions/Abbreviations	
SOP	Standard Operating Procedure
UOB	University of Bristol

SOP - 21

Device & File Encryption (mobile and storage devices)

1. PURPOSE:

To provide step-by-step instruction on encrypting mobile and storage devices.

2. REFERENCE:

- The main University site on data security, containing comprehensive guidelines to storing, handling and destroying confidential data: <http://www.bris.ac.uk/infosec/uobdata/>
Short and useful sublinks (well worth reading):
 - Working offsite: <http://www.bris.ac.uk/infosec/uobdata/offsite/>
 - Encryption flowchart: <http://www.bris.ac.uk/infosec/uobdata/encrypt/>
 - Think Twice guidelines: <http://www.bris.ac.uk/infosec/uobdata/thinktwice/>
 - Using mobile phones, tablets and laptops: <http://www.bris.ac.uk/infosec/uobdata/mobile/>

3. PROCEDURE:

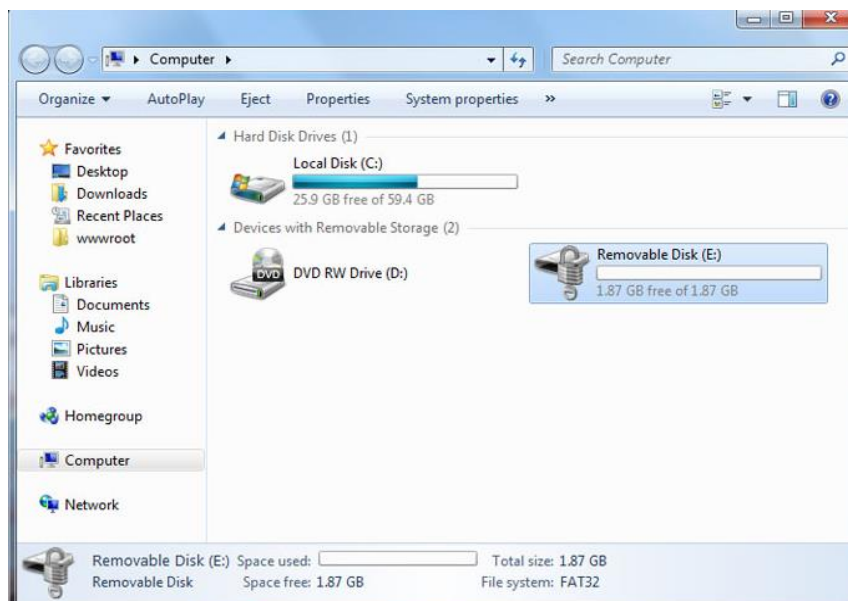
All personal information must be stored on encrypted devices. In practice this means that you must either be using a fully encrypted University laptop, a fully encrypted laptop of your own, or storing all your data on a university PC. Furthermore, all flashdrives/memory sticks used for university work must be encrypted. Finally, it is very important to lock your computer whenever you leave it unattended, as unauthorised access to our Z-drive or your personal files could constitute a data leak.

Encryption is different from having a simple password on your Windows login. Encryption is a full re-coding of the entire computer disk in a way which renders it unreadable to anyone without the encryption key.

3.1 How to:

Enabling encryption on your laptop or memory stick

To check if your laptop's hard disk, or your memory stick is encrypted. First go to My Computer; if the drive has a padlock symbol on it, as shown in the screenshot below, then it is encrypted. If the padlock is gold, then the drive is encrypted and you have not entered a password. If the padlock is silver and unlocked, then the drive is encrypted but the computer you are using knows the password needed to unlock the drive. Should the drive have no padlock, then you need to encrypt it before you can use it for storing research data.



SOP - 21

Device & File Encryption (mobile and storage devices)

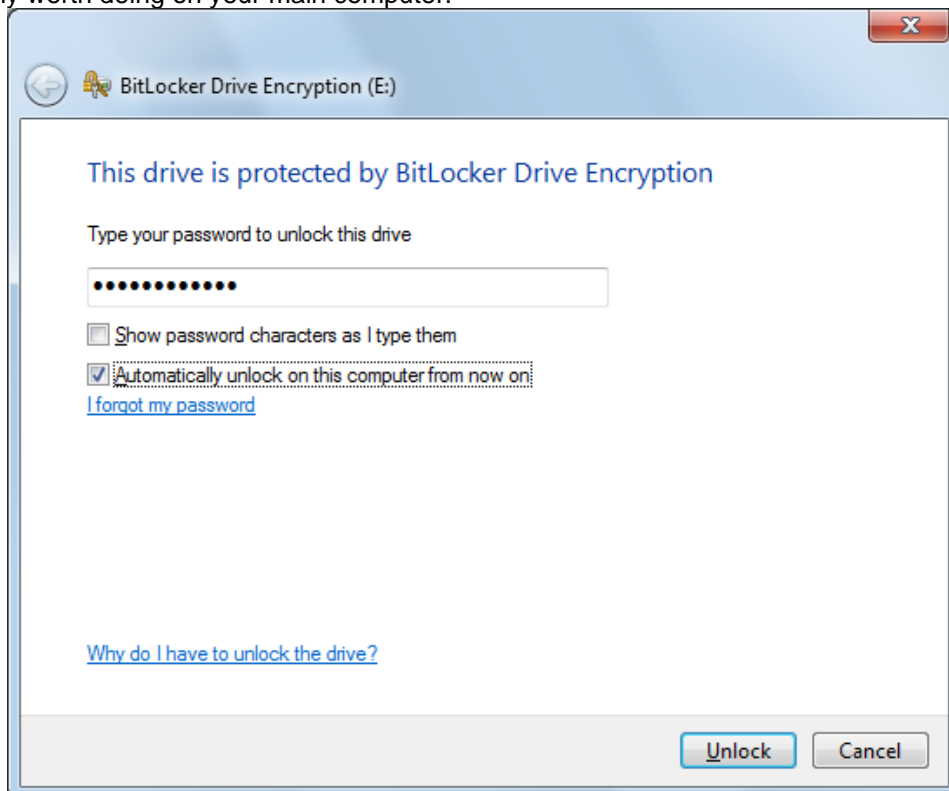
Encrypting a hard disk or USB is easy on Windows. Right click on your chosen drive. Select the “Turn on BitLocker” option and wait while the computer initialises BitLocker on your drive. You will be presented with a screen for password entry. Choose a password which you will not forget, since losing your password will mean you lose everything on the drive. However, ensure your password is strong by using unknown words and a mix of punctuation and upper and lower case letters.

A good tip for generating strong passwords is to use the first letter of every word in an easily memorable sentence. For example, “David Troy is 30 and does experiments on the shape of beer glasses”, might become “DTi30adeotsobg?”, after adding a bit of punctuation for good measure. That way, whenever you enter the password you can simply recite the sentence in your head.

After you have selected a password you are given the decision to print and/or save the recovery key. It is very important that you do not store the recovery key in the same location as the computer. Ideally you should keep the recovery key hidden, locked away and in another building/office.

Finally, the drive is ready to encrypt. Depending on the size of the drive and its contents, this could take a while. If you are encrypting your entire laptop’s hard disk, then it could take hours. Click “start encryption” and do not turn your computer off/remove the memory stick until the encryption process is complete.

Once encryption is complete you will need to enter the password to unlock the drive. On the password unlock screen there is the option for Windows to save the password so that the drive automatically unlocks; this is probably worth doing on your main computer.



For more information see:

<http://windows.microsoft.com/en-gb/windows/protect-files-bitlocker-drive-encryption#1TC=windows-7>

alternatively Information Security have comprehensive information on how to encrypt both mobile and storage devices: <http://www.bristol.ac.uk/infosec/uobdata/encrypt/>

SOP - 21

Device & File Encryption (mobile and storage devices)

4. TROUBLE SHOOTING:

Problem	Solution
Any problems	<p>Prof Marcus Munafò (0117) 954 6841 internal 46841 Marcus.Munafò@bristol.ac.uk</p> <p>Dr Angela Attwood (0117) 331 7814 internal 17814 Angela.Attwood@bristol.ac.uk</p>