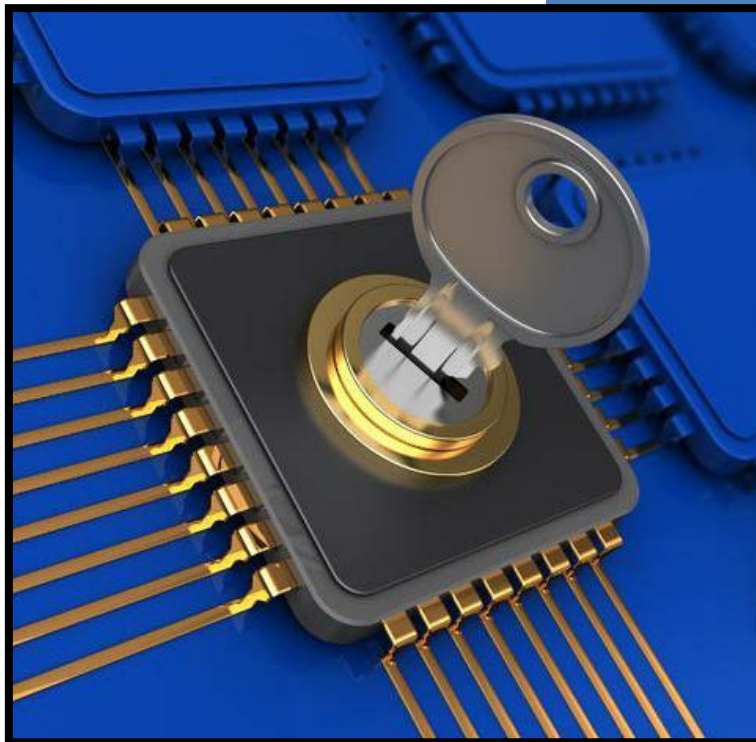


BitLocker Encryption – User Guide



This document provides guidance for users of the BitLocker Encryption software installed on University of Wolverhampton managed staff devices as part of the Information Security Project 2016/17 rollout.

Further guidance and assistance can be obtained by contacting the ITS Service Desk (ext.2000).

TABLE OF CONTENTS

Desktop BitLocker Encryption – Process	2
Laptop BitLocker Encryption – Process.....	5
Laptop BitLocker Encryption - Logon.....	9
Laptop BitLocker Encryption - Lost / Forgotten PIN	10
Contacting the ITS Service Desk.....	10
Access BitLocker Self-Service Portal	11
BitLocker PIN Reset.....	13
Shared Laptop BitLocker Encryption Process	15

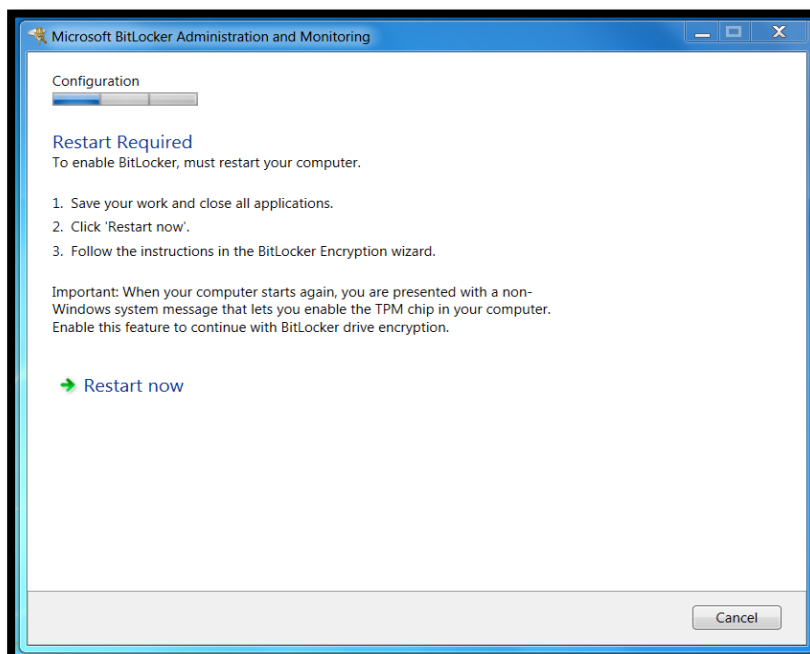
DESKTOP BITLOCKER ENCRYPTION – PROCESS

BitLocker hard drive encryption will be scheduled for activation on your device as part of a planned rollout to all staff laptops. The following screen will be displayed allowing the process to begin:



You can select the **Postpone** option to delay the encryption process, however after a period of 21 days have passed the Postpone button will deactivate and you will only have the option to start the process

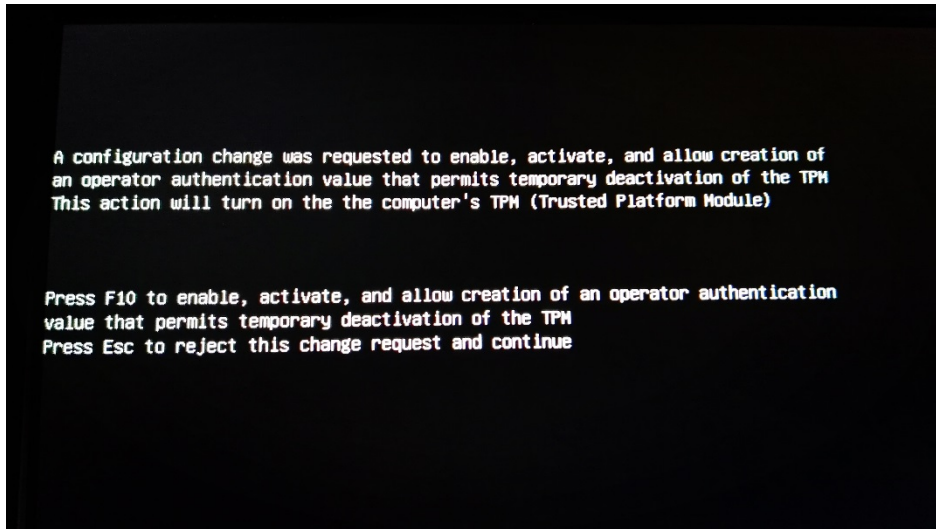
- 1) Select **Start** to commence the process and the following **Configuration – Restart Required** screen will be displayed



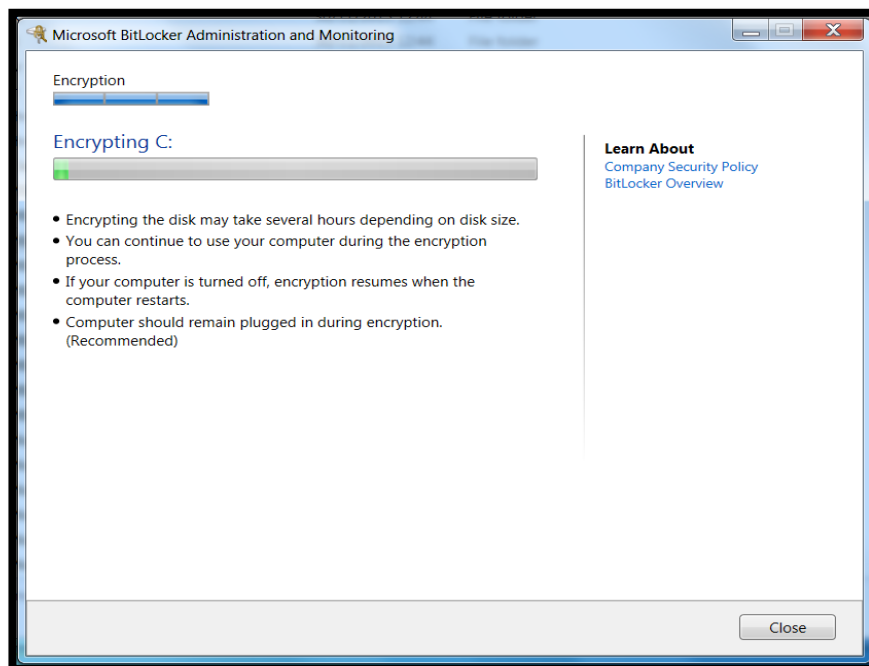
This screen tells you that when your computer is restarted you will need to enable a device change to allow BitLocker drive encryption process to continue

- 2) Select **Restart Now**

- 3) Upon a restart you **may** be presented with a similar screen to one show below, follow the instructions provided on the screen to continue the process of encrypting your device:



- 4) When you log back in the encryption process will have started for which you will be presented with the following screen:



YOU MAY

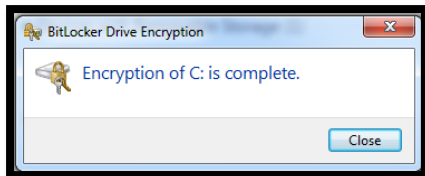
Close this window and the encryption process will continue in the background.

Continue using the device whilst encryption is taking place.

Shutdown and restart your device as required. The process will continue next time the device is

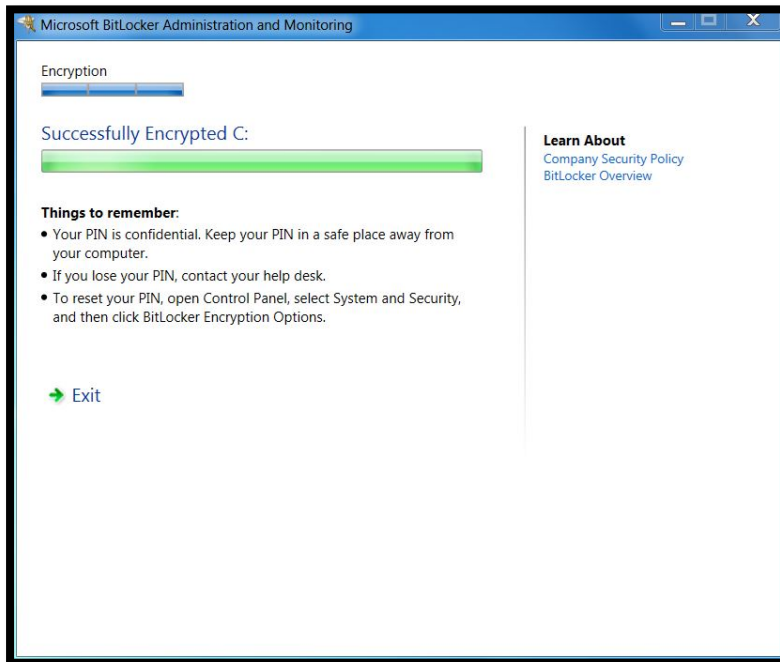
How long this takes is dependent on various factors including:

- The size of the hard drive
 - The amount of data stored on the disk
 - The age of the machine
- 5) You will see with one of the following prompts when the encryption process has successfully completed:



Click **Close**

OR

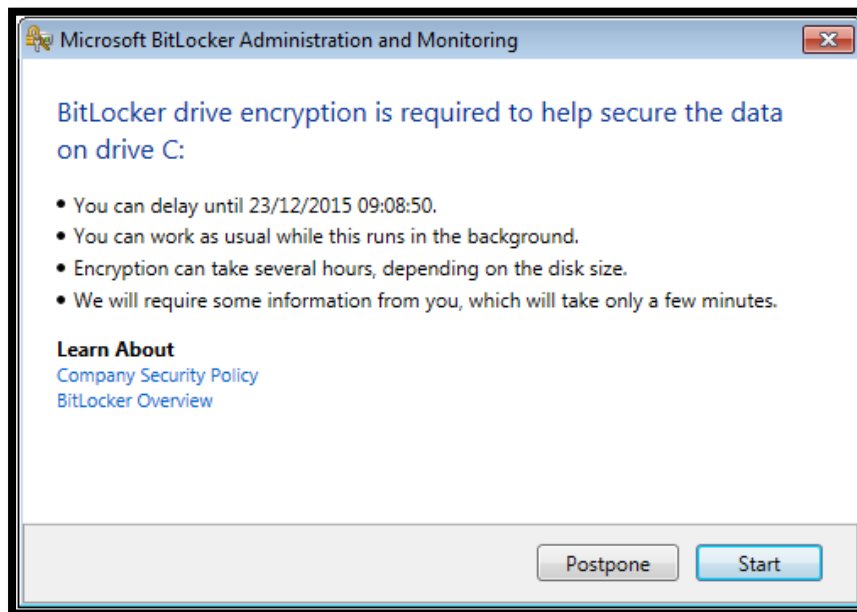


Click **Exit**

LAPTOP BITLOCKER ENCRYPTION – PROCESS

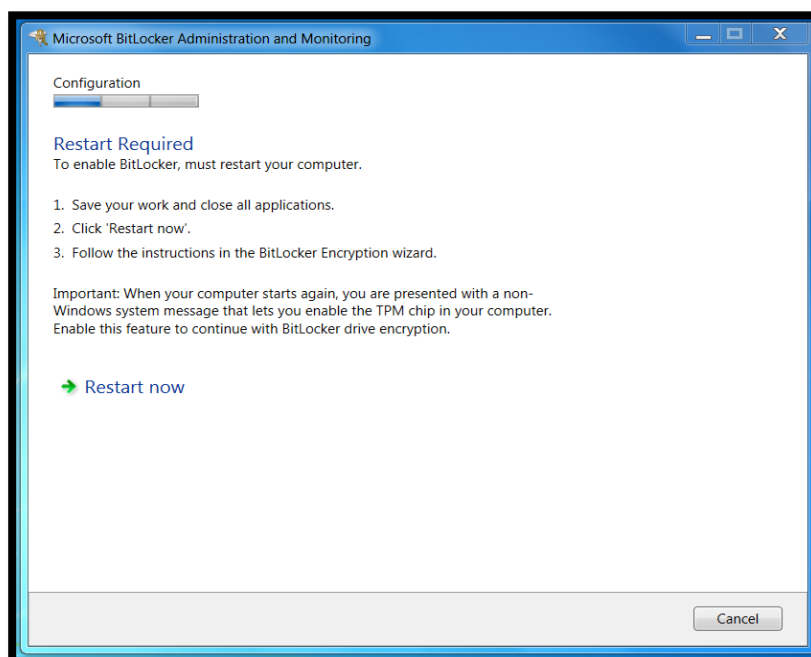
**Ensure your laptop is connected via the mains power before continuing*

BitLocker hard drive encryption will be scheduled for activation on your device as part of a planned rollout to all staff laptops. The following screen will be displayed allowing the process to begin and will appear every 90 minutes if postponed.



You can select the **Postpone** option to delay the encryption process, however after a period of 21 days have passed the Postpone button will deactivate and you will only have the option to start the process

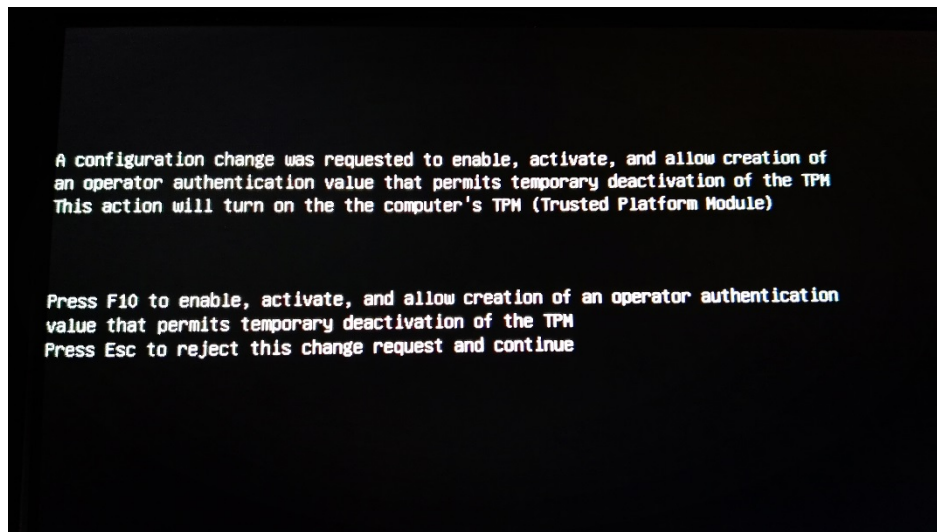
- 1) Select **Start** to commence the process and the following **Configuration – Restart Required** screen will be displayed



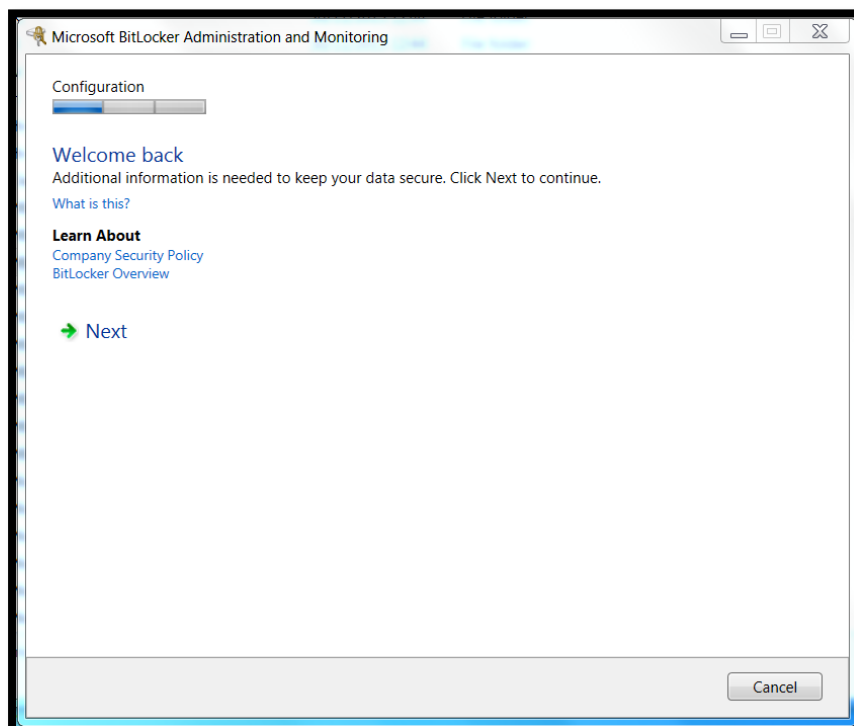
This screen tells you that when your computer is restarted you will need to enable a device change to allow BitLocker drive encryption process to continue

- 2) Select **Restart Now**

- 3) After your laptop restarts a screen similar to the following will be presented:



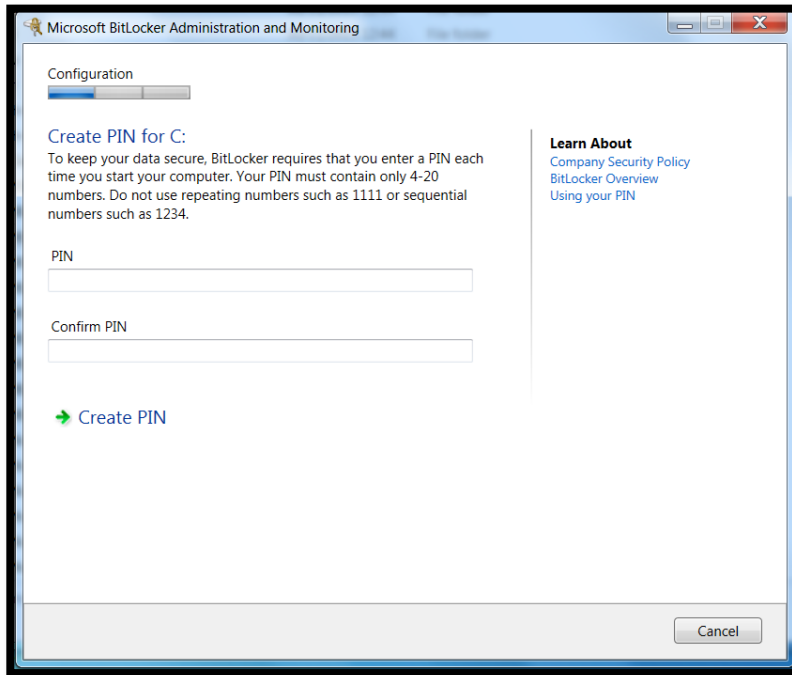
- 4) BitLocker is requesting permission to make the required configuration changes to your laptop, press **F10** to allow the changes to be made.
- 5) Your device will restart and load Windows, when it has done this log into your device as normal.
- 6) Once you have logged onto your laptop you will be prompted with the **Configuration – Welcome Back** screen:



If you would like to learn more about BitLocker there are two links provided for further information namely **Computer Security Policy** and **BitLocker Overview**.

- 7) Select **Next** to proceed

8) You will be presented with the following **Configuration – Create PIN for C:** screen:

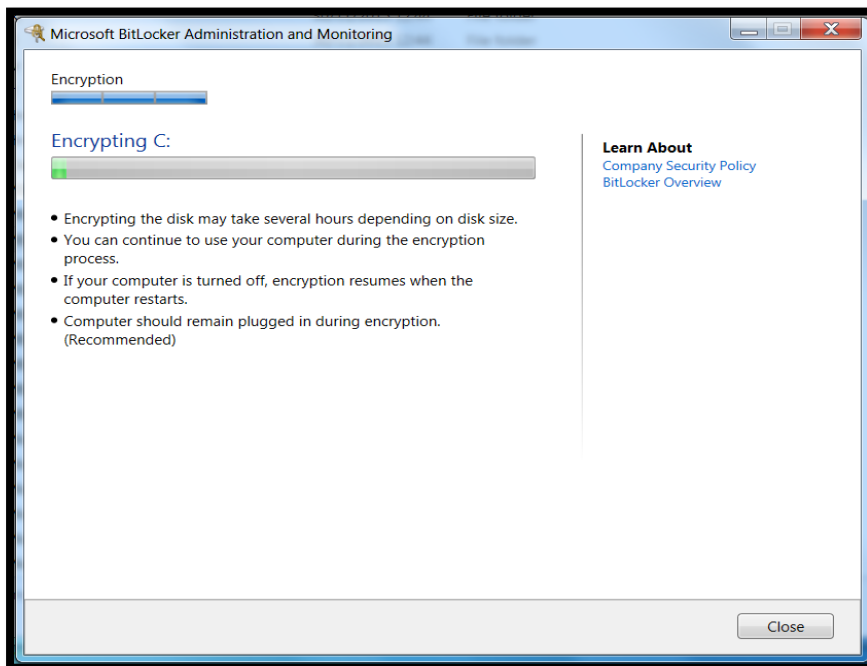


This screen will guide you in creating a BitLocker PIN

9) Please enter a numeric 4-digit PIN in both fields

NOTE: repeating numbers such as 1111 or sequential numbers such as 1234 are **NOT** allowed

10) Click **Create PIN** and the encryption process will begin as per the following screenshot:



YOU MAY

Close this window and the encryption process will continue in the background.

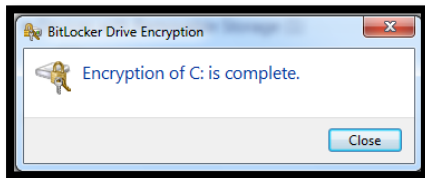
Continue using the device whilst encryption is taking place.

Shutdown and restart your device as required. The process will continue next time the device is

11) How long this takes is dependent on various factors including:

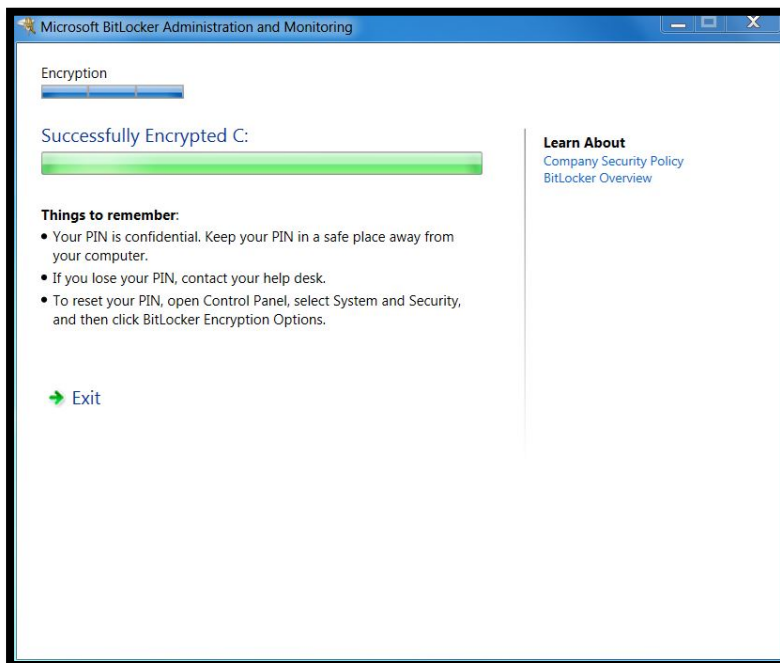
- The size of the hard drive
- The amount of data stored on the disk
- The age of the machine

12) You will see with one of the following prompts when the encryption process has successfully completed:



Click **Close**

OR



Click **Exit**

LAPTOP BITLOCKER ENCRYPTION - LOST / FORGOTTEN PIN

If you are unable to logon at this point don't worry, you will need to enter a **BitLocker Recovery Key** which you can obtain in one of the following ways:

- By accessing the BitLocker Self-Service Portal, if you have another device available to access
- By contacting the ITS Service Desk

You will be presented with the **Windows BitLocker Drive Encryption Recovery Key Entry** screen:

```
Windows BitLocker Drive Encryption Recovery Key Entry
Enter the recovery key for this drive.

____ _
____ _

Drive Label: W7N-ITR13906 OSDisk 22/06/2016
Recovery Key ID: 201CE994-85BC-4E0E-A871-2F6C34C5B24F

Use the function keys F1 - F9 for the digits 1 - 9. Use the F10 key for 0.
Use the TAB, SHIFT-TAB, HOME, END and ARROW keys to move the cursor.

The UP and DOWN ARROW keys may be used to modify already entered digits.

ENTER=Continue          ESC=Exit
```

You will need to give the first 8-digits of Recovery Key ID when you contact the ITS Service Desk or the BitLocker Self-Service portal

CONTACTING THE ITS SERVICE DESK

When you contact the ITS Service Desk requesting a recovery key for your laptop they will ask you for the following:

- Your username
- The first 8-digits of your recovery key ID (as per screenshot above)

They will give you a 48-digit code which you will need to enter as per below:

```
Windows BitLocker Drive Encryption Recovery Key Entry
Enter the recovery key for this drive.

044671 492613 045210 567831
540617 702988 432685 23838

Drive Label: W7N-ITR13906 OSDisk 22/06/2016
Recovery Key ID: 201CE994-85BC-4E0E-A871-2F6C34C5B24F

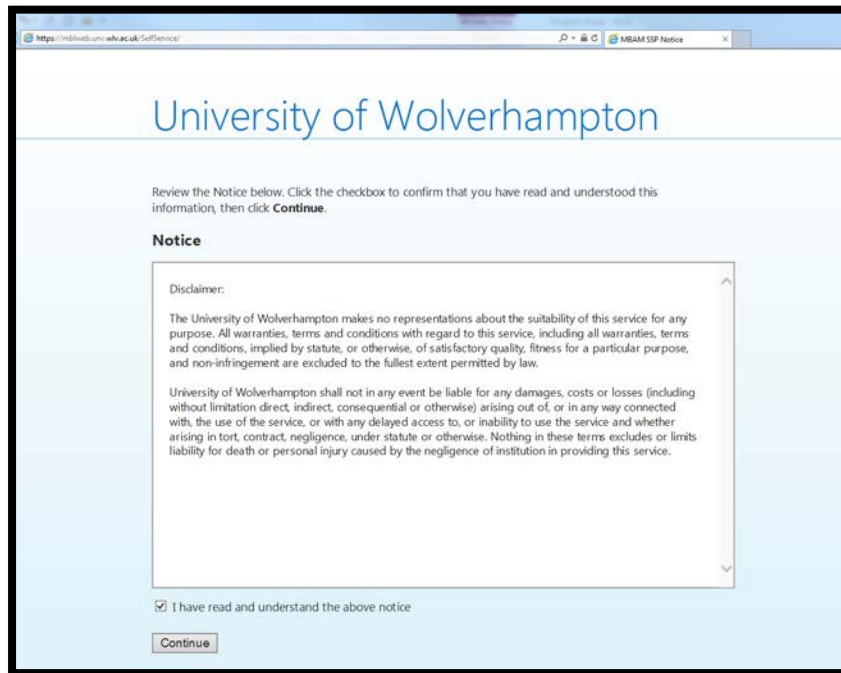
Use the function keys F1 - F9 for the digits 1 - 9. Use the F10 key for 0.
Use the TAB, SHIFT-TAB, HOME, END and ARROW keys to move the cursor.

The UP and DOWN ARROW keys may be used to modify already entered digits.
```

ACCESS BITLOCKER SELF-SERVICE PORTAL

If you have forgotten your PIN and have access to another device with a web browser, you can use the Self-Service Portal at <https://mblweb.unv.wlv.ac.uk/SelfService> to get a recover key which will enable you to access your laptop.

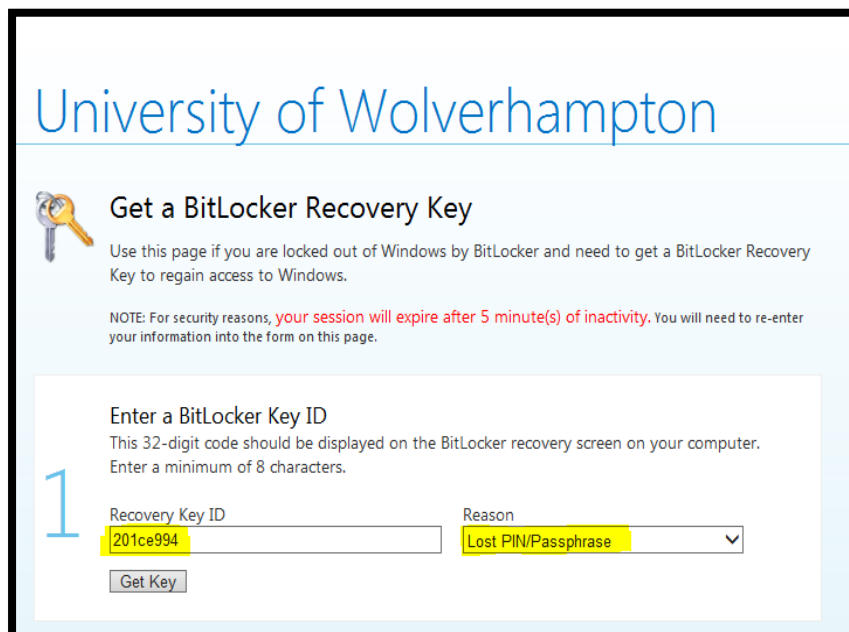
The Self-Service Portal can be accessed both on and off-campus via a Web browser.



The screenshot shows a web browser window with the URL <https://mblweb.unv.wlv.ac.uk/SelfService>. The page header reads "University of Wolverhampton". Below the header, there is a notice section titled "Notice" with a "Disclaimer" box containing the following text: "The University of Wolverhampton makes no representations about the suitability of this service for any purpose. All warranties, terms and conditions with regard to this service, including all warranties, terms and conditions, implied by statute, or otherwise, of satisfactory quality, fitness for a particular purpose, and non-infringement are excluded to the fullest extent permitted by law. University of Wolverhampton shall not in any event be liable for any damages, costs or losses (including without limitation direct, indirect, consequential or otherwise) arising out of, or in any way connected with, the use of the service, or with any delayed access to, or inability to use the service and whether arising in tort, contract, negligence, under statute or otherwise. Nothing in these terms excludes or limits liability for death or personal injury caused by the negligence of institution in providing this service." Below the disclaimer, there is a checkbox labeled "I have read and understand the above notice" which is checked. A "Continue" button is located at the bottom of the notice area.

Select I have read and understand the above notice and select Continue

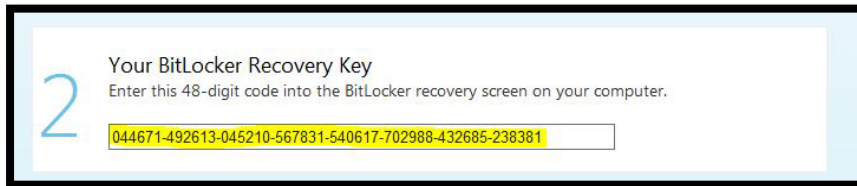
1) You will then be displayed with the Get a BitLocker Recovery Key page:



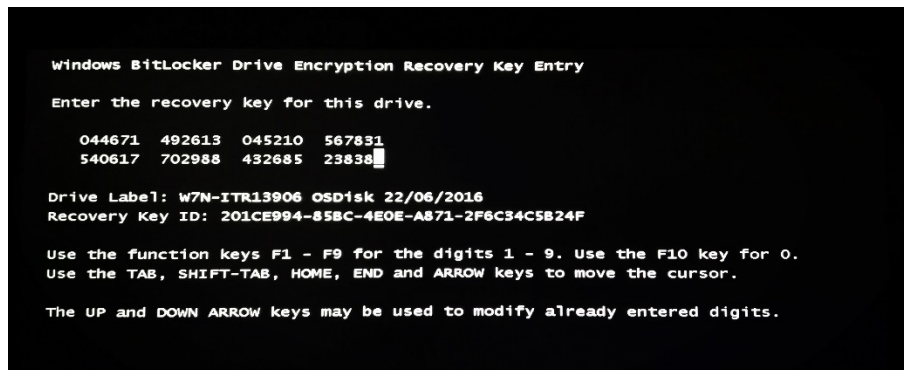
The screenshot shows the "Get a BitLocker Recovery Key" page. The header reads "University of Wolverhampton". Below the header, there is a key icon and the title "Get a BitLocker Recovery Key". The text below the title reads: "Use this page if you are locked out of Windows by BitLocker and need to get a BitLocker Recovery Key to regain access to Windows." Below this, there is a note: "NOTE: For security reasons, your session will expire after 5 minute(s) of inactivity. You will need to re-enter your information into the form on this page." The main form area is titled "Enter a BitLocker Key ID" and contains the following text: "This 32-digit code should be displayed on the BitLocker recovery screen on your computer. Enter a minimum of 8 characters." Below this text, there is a form with two fields: "Recovery Key ID" and "Reason". The "Recovery Key ID" field contains the text "201ce994" and is highlighted with a yellow background. The "Reason" field is a dropdown menu with "Lost PIN/Passphrase" selected and highlighted with a yellow background. A "Get Key" button is located below the form fields.

Enter the first eight digits of the Recovery Key ID from the device you are accessing.
Select a Reason
Select Get Key

- 2) This will create your 48-digit BitLocker Recovery Key.



- 3) Enter this code into your device at the BitLocker Drive Encryption Recovery Key Entry screen:



- 4) When you have entered the last digit of the code your device will continue to boot into Windows.

REMEMBER...!

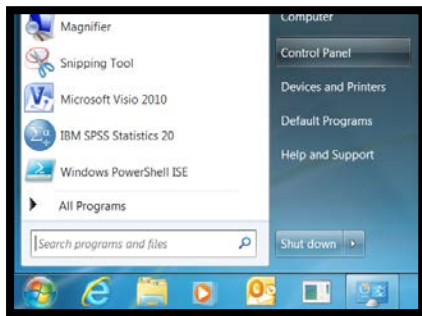
Now you have regained access to your device you should **reset your PIN** before restarting or shutting down.

Please go to the BitLocker PIN Reset section of this document

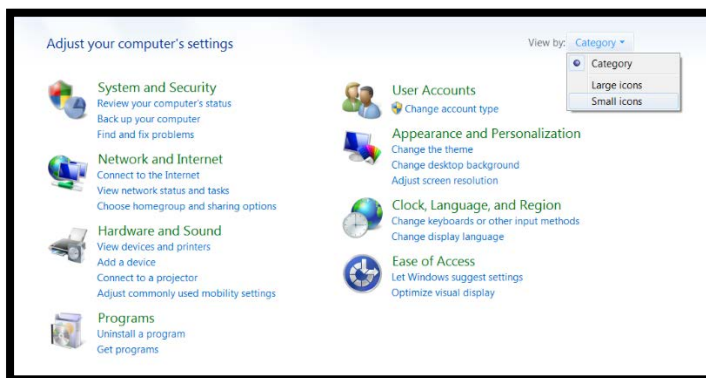
BITLOCKER PIN RESET

Resetting your PIN is a simple process with only two steps required on your laptop:

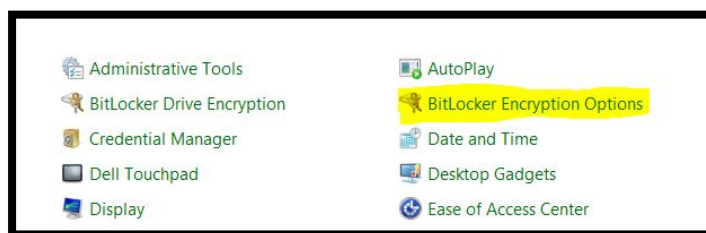
- 1) Upon successful log onto your laptop, open Control Panel by selecting **Start > Control Panel:**



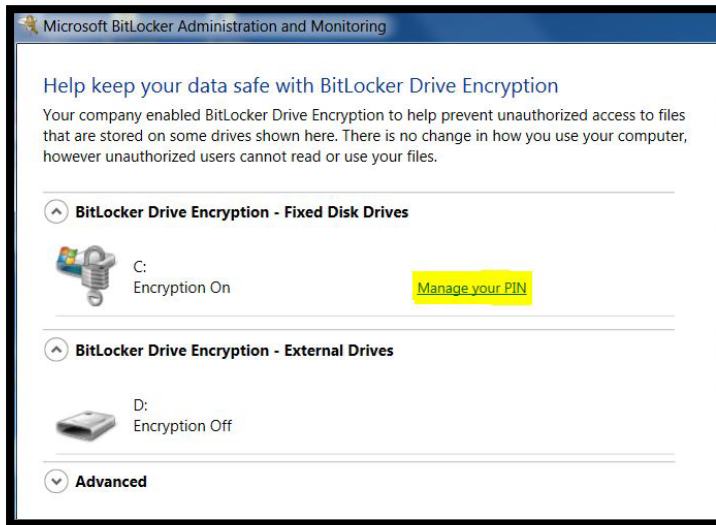
- 2) Change the view of your control panel to **small icons** if required:



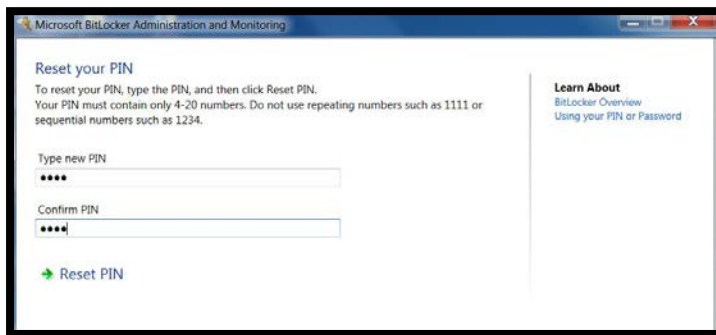
- 3) Select **BitLocker Encryption Options**.



- 4) You will see the following screen, select **Manage your PIN**.



- 5) At the Reset Your PIN screen, enter a new PIN in both fields provided and select **Reset PIN**.



- 6) Your PIN has now been reset and you will be prompted for this new PIN next time your device is restarted.



SHARED LAPTOP BITLOCKER ENCRYPTION PROCESS

Shared laptops will follow similar steps to Desktop encryption, users will be prompted to encrypt the device by following the on-screen instructions.

If a shared laptop has already been setup with a PIN from previous methods of encryption the device would need to be re-imaged to allow encryption without a PIN.

PLEASE NOTE: Users are reminded that in no circumstances should personal or commercial sensitive data be stored on shared laptops. Storage of such data on shared devices is a breach of University policy.