Technology Refresh
End User Computing

Guide 9 – Logging onto a pooled laptop

1. Mobile technology and security

This document should be read in conjunction with our council family information security staff guidelines so that you understand your responsibilities in how to safely use our information systems and follow corporate security guidelines

Our **#SafeGlasgow** section on Connect provides important information on how to keep the information you use and share each day safe and secure. Please familiarise yourself with key sections such as knowing how to report lost information and how to check for suspicious emails to prevent cybercrime.

2. Using encrypted laptops

When using a pool laptop that has been installed with encryption software you must be aware of the following.

You SHOULD NOT:

- Write down the encryption password and store in anywhere near the laptop – especially not on a label stuck to the device or bag.
- Share the encryption password with other users

You SHOULD:

- Change the encryption password when the laptop is assigned to a new user or returned to the original keeper.
- Remember to use a strong password – read our staff guide which offers top tips and examples on how to set a strong password. Avoid setting easy to guess passwords such as your pets name.)

3. Process for laptop administration

General guidance

- Pool laptops should **be locked away securely** when not in use to comply with core security policies
- You should not store personal/sensitive data stored on the pool laptop without prior approval of a senior manager who can authorise this temporarily. Once you have finished using the information it should be immediately transferred to your secure area of your file plan in EDRMS, or your shared drive on our council network, and deleted from the pool device.
- Please note that all laptops should be administered and signed out by a nominated council employee.

- When requesting the use of a pool laptop you should arrange an appointment with the dedicated member of staff who is responsible for administering it. This is so that you can be shown how to use it and how to change the encryption password. You should allow 15 minutes for this appointment.

The procedures for signing out and returning laptops are detailed below.

• Signing a laptop out

1. The dedicated member of staff handing over the laptop – known as **the keeper**, should power up the laptop.
2. On the **Windows BitLocker Drive Encryption PIN Entry** screen, the keeper must enter his current BitLocker PIN. The laptop will then boot up to the Windows 10 logon screen.
3. **The keeper** must log into Windows using their domain username and password.
4. **You** are now required to change the BitLocker PIN – refer to section 4 on **Changing your BitLocker PIN** in this document.
5. **The keeper** must now reboot the laptop.
6. Once the laptop has rebooted and on the **Windows BitLocker Drive Encryption PIN Entry** screen, you must enter your newly changed BitLocker PIN and then log into Windows using your own domain username and password. This will confirm that both the BitLocker PIN has been changed successfully and that your domain username and password has been cached onto the laptop in the event that a AOVPN connection will be used while working away from the office.
7. If you experience any issues logging in you should contact the CGI Service Desk for IT support on 0141 287 4000 or email at GlasgowITservicedesk <GCCServiceDesk@cgi.com>

• Returning a laptop

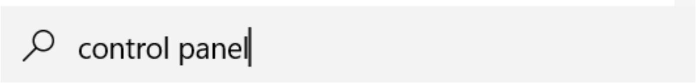
1. In the presence of the **keeper**, you should power up the laptop.
2. On the **Windows BitLocker Drive Encryption PIN Entry** screen, you must enter your current BitLocker PIN. The laptop will then boot up to the Windows 10 logon screen.
3. You must log into Windows using your domain username and password.
4. **The keeper** must now change the BitLocker PIN – refer to Section 4 in this document on **Changing your BitLocker PIN**
5. **The keeper** must now reboot the laptop.
6. Once the laptop has rebooted and on the **Windows BitLocker Drive Encryption PIN Entry** screen, the keeper must enter his newly changed BitLocker PIN. This will confirm that the BitLocker PIN has been changed successfully.
7. From the Windows logon screen the keeper can now shut down the laptop and return it to secure storage.
   - If you experience any issues carrying out this process you should contact the CGI Service Desk for IT support on 0141 287 4000 or email at GlasgowITservicedesk <GCCServiceDesk@cgi.com>

4. Changing your BitLocker PIN

If you forget your PIN or type in the wrong PIN more than 3 times your device will lock, in both cases you
should contact the CGI Service Desk to have our Bitlocker PIN reset.

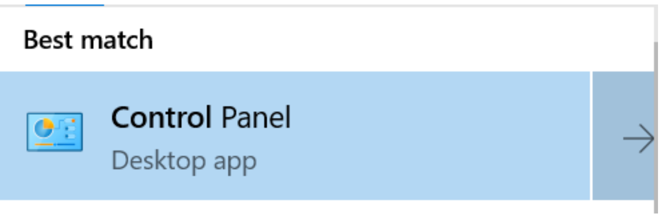
You can change your PIN by following the steps shown below:

1. Click the search bar then type **Control Panel**



control panel

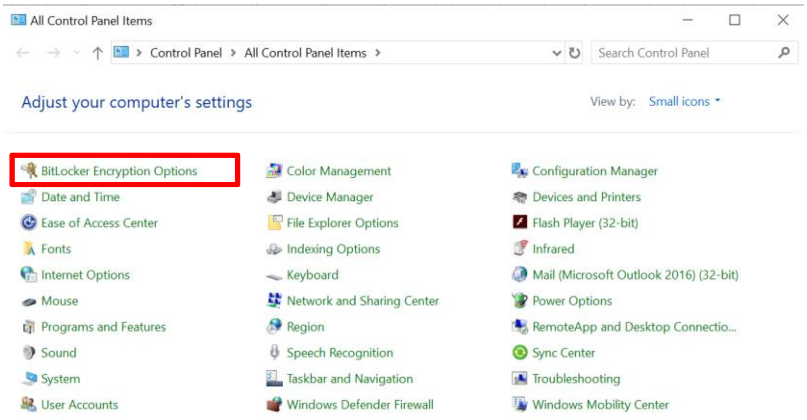
2. Click **Control Panel**



Best match

Control Panel
Desktop app

3. **Select Bitlocker Encryption Options**



All Control Panel Items

Control Panel > All Control Panel Items >

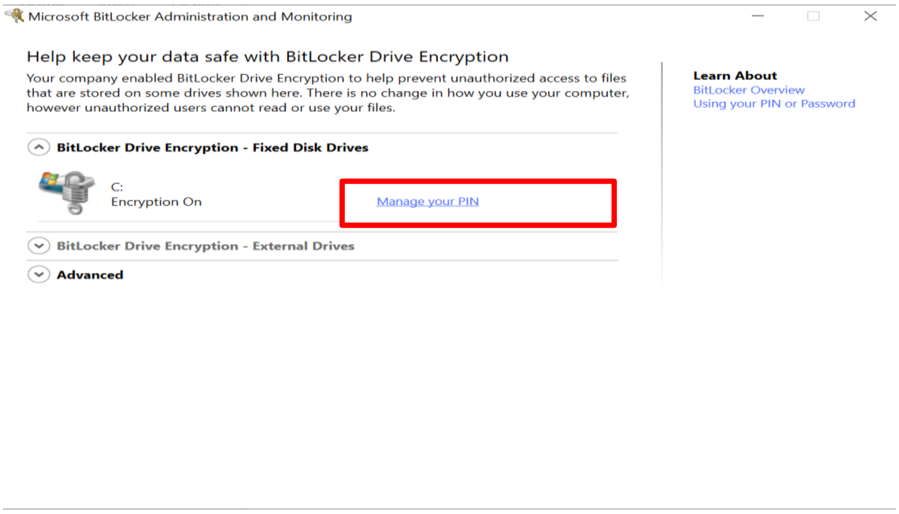
Search Control Panel

Adjust your computer's settings

View by: Small icons

- BitLocker Encryption Options
- Date and Time
- Ease of Access Center
- Fonts
- Internet Options
- Mouse
- Programs and Features
- Sound
- System
- User Accounts
- Color Management
- Device Manager
- File Explorer Options
- Indexing Options
- Keyboard
- Network and Sharing Center
- Region
- Speech Recognition
- Taskbar and Navigation
- Windows Defender Firewall
- Configuration Manager
- Devices and Printers
- Flash Player (32-bit)
- Infrared
- Mail (Microsoft Outlook 2016) (32-bit)
- Power Options
- RemoteApp and Desktop Connectio...
- Sync Center
- Troubleshooting
- Windows Mobility Center

4. On the **Microsoft BitLocker Administration and Monitoring** screen, click **Manage your PIN**



Microsoft BitLocker Administration and Monitoring

Help keep your data safe with BitLocker Drive Encryption

Your company enabled BitLocker Drive Encryption to help prevent unauthorized access to files that are stored on some drives shown here. There is no change in how you use your computer, however unauthorized users cannot read or use your files.

BitLocker Drive Encryption - Fixed Disk Drives

C:
Encryption On

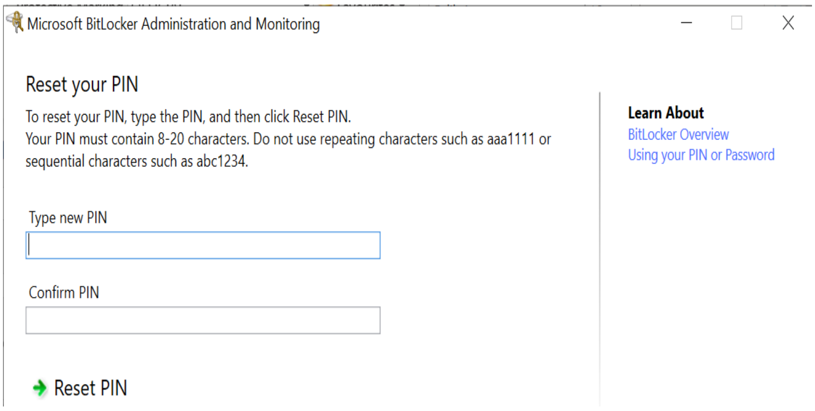
Manage your PIN

BitLocker Drive Encryption - External Drives

Advanced

Learn About
BitLocker Overview
Using your PIN or Password

5. Type your **new PIN** in both the **PIN** and **Confirm PIN** fields then click **Reset PIN**


Microsoft BitLocker Administration and Monitoring
Learn About
BitLocker Overview
Using your PIN or Password
Reset PIN

Reset your PIN

To reset your PIN, type the PIN, and then click Reset PIN.
Your PIN must contain 8-20 characters. Do not use repeating characters such as aaa1111 or sequential characters such as abc1234.

Type new PIN

Confirm PIN

***You have now reset you Bitlocker PIN**