Remote Access

What is this guidance about?
It provides users with information which can be used to create a secure and compliant work environment when accessing University information and information systems remotely.

Who is this guidance aimed at?
All users who have been authorised by the University to access, download or store University information.

Who can you contact if you require further information?
IT Service Desk on 0141 273 1234 or internal extension 1234 or https://myservice.gcu.ac.uk

Guidance
Remote access to University networks by users' needs to be managed in order to minimise security risks. To address this issue the University offers a secure remote connection called a Virtual Private Network (VPN).

VPN is a technology that creates a private, safe and encrypted connection between two computers; the computer you are using (remote computer) and the computer you are connecting to, which stores the information you require access to (host computer).

The following is a set of best practise guidance for working remotely with University information.

- The remote computer must be owned by and registered to the University; this will ensure a compliant and up to date build standard
- The remote computer and any other device (e.g. USB drive, external hard drive, CD/DVD) must be encrypted if used to store highly confidential or confidential information
- Unencrypted University owned and registered portable computer devices must not be used to download or store highly classified or classified information
- The primary or master copy of all classified information must be kept on the University's network drives
- Highly confidential or confidential information must not be copied or transferred to an unauthorised third party storage provider (cloud storage)
- Reasonable precautions must be taken to protect remote computers from theft. For example lock the device in a secure unit when not in use, device must not be left unattended if using in a public space
- When working in a pubic area information displayed on screen must be concealed from the general public
- Personally owned computer devices can be used to create a VPN and access or view University information but must not be used to download or store highly classified or classified information

Instructions on how to setup a VPN can be found at: http://www.gcu.ac.uk/staff/it/vpnaccess/

Information Security Policies: https://www.gcu.ac.uk/staff/it/itregulationspolicies/