

# Encryption

## What is this guidance about?

It provides users with information which can be used to create a secure and compliant work environment when handling and sending highly confidential and confidential (classified) information within and out with the University's networks.

## 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

Handling and sending classified information over the University network and the internet needs to be carefully managed in order to minimise security risks. It's important that users are fully aware of their responsibilities regarding information classifications and the type of device used to store, download and or send that information.

The following is a set of best practise guidance for handling and sending classified information over the University network and the internet.

- All classified information must be password protected when sent as an email attachment over the University network; the password should follow using one of the following; telephone, SMS, hand written note or further email
- All classified information must be encrypted when sent as an email attachment over the internet; the password should follow using one of the following; telephone, SMS or further email
- The portable computer device used to download, store and or send classified information over the University network or internet must be encrypted, owned by and registered to the University; for information on the encryption process please contact IT Service Desk on x1234 or at [ISTD@gcu.ac.uk](mailto:ISTD@gcu.ac.uk)
- If you're working remotely using a VPN connection and you download, store or send classified information over the internet then the remote computer must be encrypted, owned by and registered to the University
- Unencrypted portable computer devices owned by and registered to the University must not be used to download, store or send classified information over the University network or the internet
- Computer devices owned by individual members of staff can be used as the remote computer in a VPN session but cannot be used to download, send or store classified information over the internet

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