Information Services

Information Security

Guideline for safe and secure working on and off campus

1 Purpose

Purpose of this document is to provide a guideline which will enable university staff and other authorised users to work safely and securely at their place of work and out wth their place of work.

1.1 Scope

This guideline applies to University staff and other authorised users who use a fixed desktop, laptop or any other computer device to process and or store university information resources.

This guideline applies to university information which is classified as confidential and or highly confidential.

This guideline applies to university owned and configured fixed or mobile computer devices which are used to process and or store university classified information.

1.2 Contact

Direct any questions about this guideline to the IT Service Desk at ithelp@gcu.ac.uk

2 Working on Campus

The University promotes a safe, secure and tidy work area when staff and other authorised users are at their place of work.

When working on campus, all staff and other authorised users need to be aware of their responsibility to ensure the security of the information they handle, in accordance with the Information Handling and Classification Policy and for the safe keeping of University equipment.

2.1 Requirements of The Guideline:

- Be aware of people close by, when logging in to your device, when working on classified or sensitive information and when making confidential or personal phone calls; consider the use of data privacy screen filters only if your desk/screen position is exposed to passing footfall
- Screen lock your device when away from your place of work even for the shortest of time; you can lock your computer device by holding down ⊞ + L
- Ensure all external digital storage media are securely locked away; for example, USB pen drives, external storage/hard drives
- Always access your information digitally; if you need to use hard copy documents you should;
    - Handle any piece of paper only once; that is act on it, securely store it or dispose of it using the secure shredding units located throughout your work area
    - Keep only the documents you are working on at that time, on your desk
    - Securely lock away confidential and sensitive documents when you leave your desk
    - When your office/room is left unattended close and lock filing cabinets or other furniture units used to store hard copy documents
- At the end of your working day log out of your respective domain and store your laptop or other computer device in your secure personal storage unit
- Ensure that your office/room door is locked at the end of the working day

All staff and other authorised users need to ensure that they keep their place of work tidy, do not leave keys, access or ID cards on their desk unattended and carry their GCU employee ID card on them at all times during working hours.

By following this guideline all staff and other authorised users will play their part in creating and maintaining a safe, secure and tidy work area.

3 Working off Campus

When working off campus, often referred to as working remotely, all staff and other authorised users need to be aware of their responsibility to ensure the security of the information they handle, in accordance with the Information Handling and Classification Policy and for the safe keeping of University equipment.

Staff and other authorised users need to be mindful of the risks associated with the environment they work in. They must also pro-actively seek to reduce the level of that risk or if possible remove the risk entirely.

3.1 Requirements of The Guideline

- Staff and other authorised users should, at all times, minimise the amount of hard copy classified and sensitive information they take off campus and ensure it is stored securely after the work period is complete
- Never leave or store your device/hard copy information in a car or other vehicle; whilst travelling its good practise to keep university equipment/documents on your person at all times
- Only use university issued and configured devices when working on confidential or sensitive information
- Use the university VPN when working on confidential or sensitive information
- Avoid downloading confidential or sensitive information onto your local hard drive and where possible ensure that university information stays on university systems and storage
- Avoid using public Wi-Fi; if you have no option, ensure that web connections are using HTTPS or that a VPN is used when required
- When working off campus, that is at home or in a public space such as a cafe, train or library, care needs to be taken to limit the risks to university information and equipment. Working off campus increases the risk of the following:
    - Someone, including family members and friends, seeing our password or PIN and attempt to access your device; if you live with somebody who you can't share work information with then it's important to keep your device secure by ensuring the device is password lockable and only you know the password
    - Your device being stolen, lost or left behind
    - Someone shoulder surfing and being able to see the information you are working on
    - Someone eavesdropping or overhearing   a sensitive conversation; conducting a sensitive conversation in public could present and eavesdropper with an opportunity to record your conversation
- Be on constant guard against phishing emails and fake websites; do not follow links or open attachments that you are not expecting
- Treat all unexpected emails, phone calls and text messages with suspicion; even if you know the sender/caller

4 General Information and Advice

- Whilst **working off campus** you may experience a reduction in connectivity speed and stability; this is very dependent on the connection service that you are using. It will be your home network provider (Sky/BT/Virgin etc.) or a third party external network/public Wi-Fi used in cafes, trains or libraries
- Upload and download speeds may vary greatly and are not equivalent to the level of service available whilst you are **working on campus**

Staff and other authorised users of university information resources have a responsibility to apply the safeguards outlined above. Failure to do so, could put the university's information resources and equipment at risk and as a consequence, could result in an issue of potential misconduct.