Data Protection considerations when working remotely

Where you are required to have access to personal data to conduct admin, teaching or research activities this information **must** remain within the GCU data environment or on a GCU approved external environment. The easiest way to achieve this is to use the GCU Cisco AnyConnect VPN.

Maintaining security of hard copies

All staff and students are encouraged to minimise the use of hard copy data containing personal information when working remotely. Any hard copy data that is required should be treated in the same way as it would when in the office.

- Secure the data in a location that cannot be easily accessed by others.
- Shred any documents that are no longer required. If a shredder isn't available, secure the documentation until it can be returned to campus for proper disposal.
- Keep organisation data separate from personal data. This will avoid accidently keeping hold of data for longer than is necessary.

Highly sensitive datasets should remain on GCU campus to avoid potential data breaches. Consider scanning these hard copies into secure GCU network drives to review off campus where allowed.

Tips to maintain data protection standards when working remotely

- Use work provided devices to store and access information. When personal devices are used, ensure all work is conducted using the GCU VPN and saved in GCU approved systems.
- Ensure devices are encrypted and password protected e.g. laptop, mobile phone, voice recorder.
- Be mindful of confidentiality when conducting phone calls or video calls when working remotely.
- Tidy away in a secure place any hard copies and devices when not in use.
- Position screens and papers in a way that they cannot be viewed by others. In data protection family members/ house mates are third parties whom information cannot be disclosed to.
- Do not be tempted to show interesting work to others in the home. This constitutes an unauthorised disclosure.
- Follow the usual rules set out by GCU when sharing information with third party organisations.
- Further details about GCU IT remote working policy is available here.

Reporting Breaches

Example of data breaches can include but are not limited to:

- sending an email to the wrong recipient;
- accidentally disclosing personal data to an unintended party (via chain emails);
- deleting data that you cannot retrieve;
- being the victim of a phishing email scheme;
- having access to data you should not have access to

It is essential that all data breaches continue to be reported in the usual manner. If you believe there has been a data breach, log the incident through the my service portal. Further information on incident management is available here.