Working off campus

When working off campus, you can make use of a variety of services to help you stay connected wherever you are.

Page: **Connect to the VPN** — enables access to H: drive, departmental filestore and certain other IT services from off campus

Page: **Email help** — access to email is available from anywhere in the world at lancaster.ac.uk/office365

Page: **Jabber help** — allows you to make and receive phone calls on your computer, just like you would on your desk phone

Page: **LU Box help** — provides secure cloud storage. Files are accessible from anywhere via the web, mobile apps and on your PC or Mac using Box Sync. Files may optionally be shared with other members of the university and external parties.

Page: **Remote desktop help** — control your office PC from off campus

Page: **Skype for Business help** — send instant messages, make video calls, search the University directory and host online meetings

Below is a playlist of videos to help you get started with these services.

Whether you are on or off campus, you need to abide by University policy when working with University information.

Frequently asked questions

- What advice should I follow when working from home?

  While working on your device:
  
  - Ensure you have your own user account and separate accounts for family members, with password protection, on the device;
  - Encrypt your computer — instructions are available in LancasterAnswers on how to set FileVault on a Mac or BitLocker on Windows;
  - Have anti-virus installed and run updates and scans regularly;
  - Install software updates/patches regularly; and
  - Log off and shut down when finished using your device.

  When using an internet browser:
  
  - Set your privacy settings appropriately and/or apply private browsing;
  - Set your browsing history to delete temporary files, history, cookies, saved passwords and web form information; and
  - Do not choose to save your passwords on your browser.

  In terms of storage:
  
  - Unless necessary, do not print documents. If you need to do have a hard copy of any document, physically lock restricted or personal information away when not in use e.g. in a locked cabinet which only you have access to).
  - Do not keep information at home for any longer than is necessary and dispose of appropriately.

  In terms of disposal:
  
  - Information containing restricted or classified information should not be placed in an ordinary waste bin. Shred or return it to campus to dispose of via confidential waste.

  - If you are using your own personal device to work on at home and have ever stored unencrypted restricted or personal information on it, you need to secure erase the hard disk (or other media) or destroy it to ensure information is irretrievable before disposal.
What guidance is available for working while travelling?

Before you travel

- Only take home the information you really need.
- Restricted or Personal information must be encrypted on portable devices (e.g. laptops, tablets, USBs).
- If information is on a laptop, encrypt the entire laptop and therefore all contents.
- Do not remove the master copy from University — take a copy of the file and update it as soon as possible on return.
- If you make a backup of restricted or personal data on a portable device, ensure the backup is encrypted.

Whilst travelling

- Keep the information (whether paper based or electronic) in your possession. This is especially the case when using public transport — hold onto bags/laptops, and do not leave the information unattended.
- Information shouldn't be left on display in an unoccupied vehicle.
- Ensure unauthorised people do not see the information you are working on (e.g. if you are working on the train, consider if other passengers can see the information you are working on).

How can I transfer information while working off campus?

Ideally you would not take information off campus and you would access information using LU Box or VPN.

If this is not possible, information can be transferred in an alternative ways. For information transfer you could consider ZendTo (for Secure File Transfer). If you must store information on a device, ensure restricted and personal information is encrypted. Encryption provides an extra layer of protection to the information by password protecting it and converting text into a non-readable form.

Further guidance on options available for storing, transferring and disposing of information securely is available at Security of data and information.

How can I report an incident or suspected breach while working off campus?

If you believe that either a data breach has occurred or you are concerned for the security of University IT equipment and/or information, please report it.

Report an incident or data breach.