# Guidance for Students on Installing Software

To keep your data and the OU secure, all students must refer to this guidance to ensure that the software is installed and updated safely.

Although this guidance is being issued to support how you manage this software, this guidance can apply to all software you install for your studies and in your personal life.

## Action to take to install and update software securely:

- Only install the software through the verified installer and a reputable download source, such as the developer's own website or a trusted app store.

- Keep the software up to date, to keep yourself and the OU safe from vulnerabilities. Check the official software website to see what the latest version is. For Windows Devices, navigate to "Start", "Settings", "Apps", then scroll to the software and click on it – you'll see a version number. If this version number doesn't match with what you saw on the official website, you'll need to update the software.
  For Mac users, Navigate to the top-level Finder menu, then the Go dropdown. Scroll down and click on Applications. This will open a folder containing the files and shortcuts of every app you've ever downloaded or own/use by default.

- To update the software, please either download the latest version from the official website again or "Check for Updates". If updates are available, please ensure the update is installed. Some applications may include a check for updates capability, or automatic updating.

- Uninstall the software when it's no longer used or required.

  ### To uninstall software:

  Some applications will include an uninstaller to cleanly remove all traces of data.
  For Windows devices, click on "Start", "Settings", "Apps", then scroll to find the software you want to uninstall, click on it, and select "Uninstall".
  For Mac users, open "Finder", "Applications", scroll to the software you want to uninstall, click "Move to trash", then go to your trash and click "Empty trash".

- If you have been given a license key, make sure it is classified as highly confidential, you do not share it with anyone, or save it locally to your devices.

If you have any questions relating to vulnerabilities in software, please email Information-Security. (information-security@open.ac.uk)