****

**Working from Home during Coronavirus**

Due to the coronavirus many employees are working from home for the first time and others are working from home on a regular basis rather than on ad-hoc arrangements. This guidance is aimed at providing a suitable environment for the handling of information, it does not cover:

* Staff wellbeing when working at home
* Supporting and line managing staff working remotely.

**Staff should:**

Consider a space, free from interruptions that provides you with the technology aids you require.

Access information using the Remote Access, VPN services or other authorised services provided by Leeds Beckett University.

Set a strong password on all devices and/or applications including your home network/WiFi router, see [IT Security webpage](https://www.leedsbeckett.ac.uk/staffsite/services/it-services/it-help/it-security/) for further information.

Use this [password checker](http://www2.open.ac.uk/openlearn/password_check/) to test the strength of your password.

Only use devices, systems and applications authorised by the university, this includes the use of cloud services.

Update browsers and anti-virus software to the latest versions.

Avoid using outdated non-secure technologies to transfer information.

Visit the [Data Protection webpage](https://www.leedsbeckett.ac.uk/partners/compliance-legal/data-protection/) further information on the data protection principals and reporting an information breach of personal data.

Ensure you have completed the on-line mandatory training on Data Protection and IT Security Training within the last three years.

**Staff should avoid:**

Downloading Personable Identifiable Information onto personal devices or your PC Desktop.

Leaving printouts in places accessible by others, especially if it contains sensitive and confidential data.

Using USB sticks and other external devices used for storing information.

Transferring information by email attachments where there is an alternative safer method.

Leaving the workspace when you are still logged-on.

Sharing your passwords with household members or writing them down.

Leaving information and devices in view, for example; house or vehicle windows and glass doors.

**Quick Checklist for managing your home workspace:**

Can the work area be overlooked, don’t forget windows?

Can you create workspace privacy by closing the door and preventing unintended interruptions?

Do you have access to a lockable unit, who has access to the keys?

If working with sensitive and/or confidential information are you operating to a clear desk policy?

If you share devices is the clear desk policy applied to the electronic desktop.

Do you need to print, is there a shredder available?

Are you likely to have sensitive discussions, who is in hearing range?

Are technical hardware and cloud services protected by adequate passwords, encryption and anti-virus software?

**[Cyber Security](https://www.ncsc.gov.uk/)**

The National Cyber Security Centre (NCSC) has warned the public to be on their guard against cybercriminals exploiting the Coronavirus (COVID-19) outbreak. Criminals have spread malware via emails purporting to contain important updates about the COVID-19 outbreak. We appreciate the these are challenging and fast moving times, but we must ask users to remain vigilant and watch out for suspicious emails and other threats.

For further information students should visit the [Library Webpage](https://libguides.leedsbeckett.ac.uk/passwords_and_digital_security/phishing) and staff should visit the [IT Security webpage](https://www.leedsbeckett.ac.uk/staffsite/services/it-services/it-help/it-security/).