THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE

Operational

Managing Personal Data Off Campus

Guidance for staff and students

This guidance is intended for all professional staff and researchers (including students) that work at home or off site, either on an occasional or a regular basis. It applies to anyone undertaking administrative, research or teaching-related work at home.

This guidance gives general advice on the issues you need to consider ensuring that any School information you work on at home is protected from loss or unauthorised access and exploitation, while also ensuring that it is accessible to anyone that needs to use if for their work. It applies to information in all formats, including paper files, electronic data, word processed documents and e-mails.

Data Protection and Freedom of Information

The Data Protection Act 1998 and the Freedom of Information Act 2000 apply to all information that you receive and create as part of your employment or research with the School, regardless of where you work or store that information.

The Data Protection Act permits people to see information that the School holds about them while the Freedom of information Act will give people the right to access any other recorded information that the School holds. The Data Protection Act also requires us to hold information about living identifiable individuals for no longer than is necessary, to ensure that information is accurate, and to adopt appropriate security measures for this information to protect it from unauthorised access, amendment or deletion.

Access and storage of information

It is best to use the Remote Desktop or a VPN to access School systems directly, rather than carry copies of information on your hard drive, usb/memory sticks or other storage devices. Using these access methods will mean that when you work at home you probably will not need to take any measures with regard to electronic information and your principal concern will be to protect your paper based information. Web access to email and to OneDrive and SharePoint is also a good way of accessing information without downloading it onto your PC.
If you are unable to use Remote Desktop or a VPN, the primary copy of School information should not be stored at home, so School records should be updated as soon as possible with copies of any work that you do at home. This applies to all research, teaching or administrative work. This allows anyone who needs to refer to the records in your absence to be able to access the most up-to-date information. It will also ensure there is a backup copy of the work, if you were to lose your work at home. Finally it will enable the School to respond to any Freedom of Information or Data Protection request for that information without having to ask you to search information you have at home.
You will need to take reasonable measures to protect the information from unauthorised loss, access or amendment whilst stored at home. This means: locking the device when you are not using it; making sure you do not share your password with others, including members of your family; and making sure that anti-virus software is always up to date and that any security patches are installed.
Any mobile devices like phones and tablets that you use to access School information should be at the very least passcode protected and, where possible, set up to be wiped remotely.

Potential security hazards

Paper

The paper information you use at home is most vulnerable to loss or unauthorised access in the following ways:

- As a result of leaving papers in household areas where they may be seen by other members of your household or by visitors. This is most likely to cause difficulties when the information is about identifiable individuals.
- As a result of crime e.g. theft.
- As a result of loss, particularly on the journey to and from work. Remember to check as you leave a vehicle or public transport that you are carrying everything with you.

All paper information must be held securely within the home environment, for example, in locked filing cabinets or boxes.

Electronic

Unless you work directly via Remote Desktop or a VPN, the electronic information you work on at home is vulnerable to loss or unauthorised access or amendment in two ways:

- Physically, through the loss, damage or access to the computer or storage medium on which the record is held, most commonly loss of flash drives or unprotected security access on home computers. It is recommended that you create an account on your home PC, use it exclusively for work and password protect the account so that accidental access by other household members is avoided. Such accidental access has been fined as a security breach by the Information

Commissioner's Office.

- Remotely, through someone accessing (hacking) your computer while it is connected to the Internet or through a virus. Anti-virus software is preloaded onto all university equipment and can also be installed on home devices.

You should also ensure that your hard drive is encrypted, particularly for devices that are regularly in transit. IMT can help in setting this up for you.

Disposal of Home PCs/Devices

If you have used your home PC to work on sensitive School information or information about living, identifiable individuals (such as raw research data), when you dispose of the computer you must make arrangements to ensure that the sensitive information is no longer accessible. Please see the guidance on destruction and disposal of mobile devices, which covers sanitisation of these types of information.

Non School email accounts

You should use the School provided email account for all School related business. If you do go outside the School's systems you would still have to provide the information for a Freedom of Information request.

Review schedule

Review interval	Next review due by	Next review start
3 years	31/10/2021	01/10/2021

Version history

Version	Date	Approved by	Notes
1	4/10/2018	GDPR WG	

Contacts

Position	Name	Email	Notes
Information and Records Manager	Rachael Maguire	r.e.maguire@lse.ac.uk	

Communications and Training

Will this document be publicised through Internal Communications?	~~**Yes/**~~ **No**
Will training needs arise from this policy	~~**Yes/**~~ **No**
If Yes, please give details	