Clear Desk and Screen Policy

1. INTRODUCTION

1.1 Purpose

1.1.1 Keele University is committed to preserving the confidentiality, integrity and availability of its data. Hardcopy data left unattended on a desk is at risk of being compromised. If a computer is left unattended and logged on an unauthorised individual could be able to access Keele IT systems and data.

1.1.2 Information security is everybody's responsibility. Keele has a responsibility to ensure that the appropriate operational and technical solutions are in place to assist in preventing data breaches from occurring. This policy fulfils a part of that responsibility.

1.1.3 However, you are have a personal responsibility to keep the data and information you access, process and delete safe and secure. Should the personal data you access or in your possession be lost, stolen or compromised it will constitute a breach of the Data Protection Act 2018/GDPR. In the event of a breach, you will have to demonstrate that your actions leading up to the theft, loss or compromise were reasonable.

1.2 Scope

1.2.1 This guidance applies to anyone who processes University data including staff, Post Graduate Researchers (PGRs), students, visitors and contractors. The guidance applies to individual as well as communal offices. Confidential data is any data that if it were compromised could have an adverse effect on the reputation of the University or the ability of the University to function.

2. POLICY

2.1 Clear Desk

2.1.1 If working in a single lockable office, when leaving our desk or workstation unattended please ensure that any confidential, personal or sensitive information is not viewable from the door or the window and that the door is locked whilst you are away. If you are going to be away from your office for more than 30 minutes you should ensure that the paper records are locked away in a drawer or cabinet and your door is also locked. Your computer screen must always be locked (see section 2.1.7) when you are not using it.

2.1.2 If you work in a shared office, e.g. 2-4 people, the guidelines for an open plan office should be observed as you alone are responsible for the data and information you are processing therefore you must ensure that it is safe and secure when you are not at your desk or workstation. Do not expect your colleagues to do this for you.

2.1.3 If working in an open plan office, ensure that paper records containing confidential, personal or sensitive personal data are secured in a locked drawer or a filing cabinet at the end of the day or if your workstation is to be unattended for a period of 5 minutes or more. Your PC or Laptop must be locked (see section 2.1.7) at all times when you are not using it.

2.1.4 Always shred hardcopy documents containing personal data or cross-shred, where possible, confidential or sensitive personal data when they are no longer required. Please don't dispose of paper records containing confidential, personal or sensitive personal data in general waste or recycling bins. Conversely, do not put general waste in the confidential bins or bags.

2.1.5 Where shredding may not be practical e.g. bulk document destruction, the University has a confidential waste process which should be adhered to:

https://www.keele.ac.uk/estates/energyenvironment/environmentalgoodpractice/
(under the section titled 'What is classed as Confidential Waste?')

Where confidential waste bags are used they should not be left unattended in open or unlocked offices.

2.1.6 Consult the University's retention schedule and destroy any hardcopy records that no longer need to be retained or when they come to their end of life.

2.1.7 Lock your screen when you leave your computer unattended:

- **For Windows devices**: Press Ctrl, Alt and Delete keys simultaneously and then ENTER or Press the windows button (between the Ctrl and Alt keys) on your keyboard and L simultaneously

- **For Macs running macOS Mojave:** go to the Apple menu and choose Lock Screen or press **Command+Control+Q**. This will lock your Mac and return you to the Login screen

- **For Macs running earlier operating system**: press **Control+Shift+Power** button (or **Control+Shift+Eject** if your Mac has an optical drive). It will lock the screen.

2.1.8 Do not write down passwords or other restricted account information on paper or post-it notes and then display them in an accessible location. Passwords must be committed to memory or if it is absolutely necessary for them to be written down, stored in a secure location and out of sight at all times.

2.1.9 Make sure that removable media is locked away when not in use. Please do not leave CDs, DVDs and Memory Sticks in drive bays, USB drives or plugged into devices.

2.1.10 Always remove documents containing confidential, personal or sensitive personal data immediately from printers.

2.1.11 Always ensure that keys to locked filing cabinets or drawers are kept in a secure location.

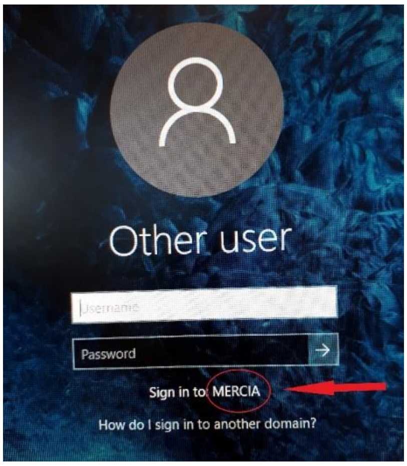
2.1.12 Do not leave confidential information in shared conference facilities or meeting rooms.

2.1.13 Remove all information from flipcharts and wipe down whiteboards.

2.1.14 Ensure that all office areas are secured when not in use. There should be a "last person out" routine so that everyone understands their responsibilities for locking doors, closing windows and setting security alarms.

2.2 PC's and laptops

2.2.1 Check that the automatic screensaver is activated after 10 minutes of inactivity. If your device is on the Keele domain this will be set up automatically for you. To check if your device is on the domain; when logging on check for the word Mercia on the screen. The following image is from a Windows 10 desktop PC:

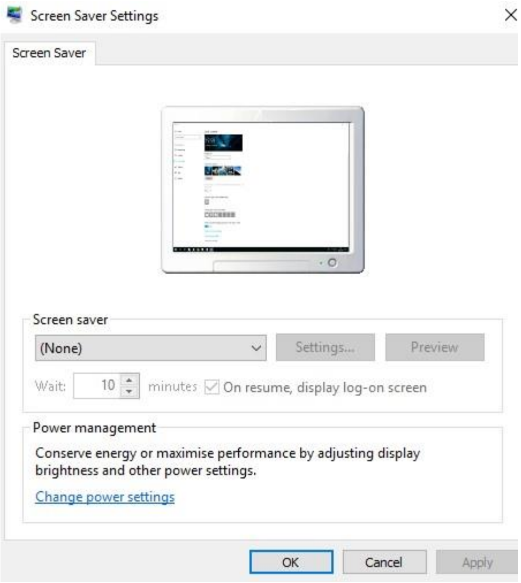


If you have a Windows 7 machine, Mercia may be displayed in the userid field.

2.2.2 For those devices that are not on the domain you must set the screen saver to activate after 10 minutes.

To do this on a Windows 10 device:

- Right-click the desktop and choose Personalize
- Click on Lock Screen and scroll to the bottom of the next screen
- Click on Screen saver setting
- From the Screen Saver drop-down list, choose a screen saver
- Use the arrows in the Wait xx Minutes text box to set the number of inactivity minutes to 10 minutes before displaying the screen saver
- Click the Preview button to preview your screen saver of choice. ...
- Click to stop the preview, click OK, and then click the Close button



Screen saver: (None)

Wait: 10 minutes ☑ On resume, display log-on screen

Power management

Conserve energy or maximise performance by adjusting display brightness and other power settings.

2.2.3 Make sure that you shut down your computer at the end of the working day.

2.2.4 Ensure that if you use a laptop or other portable computer device that it is locked in a secure location at the end of the workday.

2.2.5 When travelling with a laptop please adhere to the Mobile Device guidance: https://www.keele.ac.uk/informationsecurity/encryption/mobiledevices/

2.2.6 Always be aware when accessing confidential, personal or sensitive personal data of anyone who may be able to view the information displayed on your screen.

2.2.7 Delete any electronic data from the recycle bin of any communal computers that you use.

2.3 Summary – the 3 P's

2.3.1 **PLAN** first thing in the morning. Keep just the things you need for your workday on your desk. Start each day with a few minutes of planning so that you can organise the documents you need for immediate work. File all other folders and documents.

2.3.2 **PROTECT** information whenever you leave your desk. You obviously have to leave your desk to attend meetings or to take breaks. But whenever you do, make a quick check to see if there is sensitive information on your desk and place it inside a folder or off your desktop. And for additional security, make sure to lock your screen:

- <Windows button> and <L> (Windows)
- go to the Apple menu and choose Lock Screen or press **Command+Control+Q**. This will lock your Mac and return you to the Login screen. (For Mac running macOS Mojave)
- press **Control+Shift+Power** button (or Control+Shift+Eject if your Mac has an optical drive). It will lock the screen. (For Mac running earlier operating system)

2.3.3 **PICK UP** at the end of the day. When you leave your desk in the evening, don't leave documents on it. In order to maintain the security of both your client and employee information, it's essential to file your documents or lock them up, if necessary. If you get into the habit of clearing your desktop every day before you leave, you'll enjoy the added productivity benefits that come with a clean office first thing in the morning.

3. ROLES AND RESPONSIBILITIES

3.1 Contact

3.1.1 If you require further advice or you are in doubt about any of the contents of this guidance and what is expected of you raise a support call with the IT Service Desk or speak to your line manager. If you need advice about implementing any of the technical controls that are referred to in this guidance raise a support call with the IT Service Desk. https://servicedesk.keele.ac.uk/

3.2 Monitoring

3.2.1 Implementation of this policy will be undertaken by the Information Governance multi-institutional team consisting of the IG Champions, Information Security Manager, Data Protection Officer and the Legal & Governance Support Officer.

3.2.2 Monitoring may take the form of unscheduled sites visits during and after normal working hours.

4. RELATED POLICIES AND PROCEDURES

4.1 Policies and guidance

4.1.1 This policy should be read in conjunction with the:

- Mobile Device policy
- Data Classification and Handling Guidance

4.2 Framework

4.2.1 This policy forms part of the Information Governance Framework developed by the Data Protection Officer and the Information Security Manager. Further information can be found at: https://www.keele.ac.uk/informationgovernance/fortheuniversity/

5. REVIEW, APPROVAL & PUBLICATION

This policy will be reviewed every three years by the Information Security Manager with any changes ratified by the Information Governance Group before final approval by UEC.

6. ANNEXES

None

7. DOCUMENT CONTROL INFORMATION

Document Name	Clear Desk and Screen Policy
Owner	Simon Clements – Information Security Manager, Information and Digital Services Directorate
Version Number	Final v1.0
Equality Analysis Form Submission Date	Not required
Approval Date	19th February 2019
Approved By	UEC
Date of Commencement	19th February 2019
Date of Last Review	Not applicable as new policy elevated from a guidance document previously approved by UEC
Date for Next Review	19th February 2023
Related University Policy Documents	Mobile Device Policy Data Classification and Handling Guidance
For Office Use – Keywords for search function	