Version 1.0
6 Nov 2015

The University of Nottingham
UNITED KINGDOM · CHINA · MALAYSIA

Guidance Document: Clear Desk Routine

Maintaining a clear desk or workspace is important to help ensure information is not breached when you are at your desk, when you leave your desk unattended during the day, when you leave at night and especially when you go on holiday. This is especially important in an open plan office environment.

As part of a growing commitment to ensuring better security of our data, this guidance should be followed by all staff. The term 'restricted' in this document is used generically for all sensitive, confidential and personal data types.

Clear Desk Routine

Restricted Documents

- ✓ Never leave documents lying around in the copy, printer or fax area.
- ✓ Do not leave restricted documents or storage devices lying around on your desk for others to view. Ensure they are securely locked away when not being used and at the end of the day.

Lockable Storage

- ✓ File cabinets and other lockable storage should be kept closed and locked when not in use or when not attended.
- ✓ Keys used for access to restricted information must not be left at an unattended desk.

Information Disposal

- ✓ Never throw restricted information in the general waste or recycling bin. Ensure all restricted information is securely disposed of.
- ✓ Don't put general waste in for confidential shredding. Whilst the confidential waste disposal service is a cost free service to schools and departments it still costs the University as a whole. If you have small volumes of confidential waste shred using your own shredding machine

User Credentials

- ✓ Do not write down usernames, passwords or any other restricted account information on paper or post-it notes and post in your workspace which others could view. Commit this information to memory, or ensure this information is locked away and out of sight at all times
- ✓ Create unique passwords and change them routinely
- ✓ Never share a user account or a password

Computers and Laptops

- ✓ Always lock your computer when leaving, to avoid anyone accessing your computer, the information stored on it and your email, even if it is only for a short while. (Ctrl+Alt+Del)
- ✓ Computer workstations should be shut completely down at the end of the working day. WakeMyPC still can access all university computers even when they have been turned off.
- ✓ Lock away portable computing devices such as laptops and tablets.

Removable Storage Media

- ✓ Do not leave removable storage media such as CDs, DVDs and USB drives in drive bays, plugged in or lying around. Ensure all removable media is locked away when not in use and that all restricted information stored on removable media is appropriately encrypted.

Meeting Rooms

- ✓ Never leave restricted information behind in shared conference facilities or meeting rooms, so that it is not exposed to anyone using the room after you.
- ✓ Remove all information from flipcharts and the room, and wipe down whiteboards.
- ✓ Delete any electronic information within the recycle bin before you log off communal computers.

Office Access

- ✓ Lock all office areas when they are not in use.
- ✓ Ensure you adopt a 'Last person out' routine so that everyone understand their responsibilities for locking doors, windows and applying any security alarms on their way out.