**Department of Paediatrics Secure Working Policy**

This policy defines the DoP’s approach to ensuring work areas and devices are kept secure. All members of the department are accountable for the security of the data they have access to or have in their possession. It is vital that safety measures are followed to reduce risk to data irrespective of whether a staff member is working onsite or offsite. In the event of a data breach, it is important that all users involved can demonstrate that their actions leading up to the compromise were reasonable and appropriate.

**Expectations**

The DOP recognises that material left unattended is more susceptible to damage, disclosure, or theft. It is vital that all members of the DoP commit to meeting the following expectations for best working practices.

**1. Work space**

Confidential and sensitive information should be removed from desks and locked in drawers or filing cabinets when a workstation is not in use or is unattended for any length of time. When working offsite, it is important to maintain a similar level of privacy as you do when working onsite. For example, please carefully consider where your computer screen is located to ensure its not visible to others.

Passwords and other restricted information should not be written on sticky notes and posted in accessible locations. Where possible, users should consider using a password manager such as LastPass or KeePass to generate and store long, random, complex passwords. Please see the University’s guidance on password management for more information.[[1]](#footnote-1)

**2. Lockable Storage**

Staff should ensure that paper records containing confidential, personal, or sensitive data are secured in a locked drawer or a filing cabinet at the end of the day or if their workstation is to be unattended for any length of time. Staff must ensure that keys to locked filing cabinets or drawers are kept in a secure location.

**3. Screen locking**

Information can be viewed by unauthorised users if left on an unlocked, unattended computer screen. Screens must be locked whenever a screen is left unattended[[2]](#footnote-2).

**4. Remote Working**

It must be ensured that the same guidelines are followed when working away from the office, including at home. It is important to use systems and software that have been approved for use by the University of Oxford for University data. These systems have been assessed for security by the University and have met information governance specifications.

**5. Removable Media**

All removable devices should be encrypted. All removable media devices, including laptops and mobile phones containing sensitive data, must be stored within a secure room or locked cupboard when not in use. Removable media such as hard drives and USB sticks must not be left unattended in plain sight. When working on laptops, users should consider using a docking station or laptop tether. These are non-invasive tools which easily lock your laptop to your desk and provide security. They do not require any device modifications.

**6. Printers, Scanners, and Fax Machines**

Copies and printouts must be removed immediately from copiers, scanners, and fax machines.

Most printers within the department use Papercut, which ensures printed documents will not sit uncollected on the printer, as jobs will only print when released by the user.

**7. Shared Areas**

Confidential information and removable devices must not be left unattended in shared facilities or meeting rooms. All information must be removed from flipcharts and whiteboards at the end of meetings. Sensitive paper documentation that is no longer needed must be disposed of properly in the secure lock bins or shredded. Sensitive documentation must not be placed in confidential waste bins and not the normal paper waste bins.

**Examples**

|  |  |
| --- | --- |
| **Don’t** | **Do** |
| Write passwords on sticky notes left in workstation area | Use a password manager |
| Leave sensitive information in printer when printed | Collect paperwork immediately or use Papercut system to ensure paperwork is only released when user arrives. |
| Leave your computer screen unlocked when away from workstation | Always lock your computer screen. For Windows machines, hold down Windows key and press “L” or select the “start” button, then select your Windows account profile picture icon and choose “lock screen”. For Macs, click on the Apple icon and then select “lock screen”. |
| Leave sensitive documents such as participant or patient data, CV’s, financial documents on desk overnight | Ensure that paper records containing confidential, personal, or sensitive data are secured in a locked drawer or a filing cabinet at the end of the day. Confidential data should be locked away even when kept in private, lockable offices. |

**Monitoring compliance**

To ensure compliance with this Policy, the Information Governance Unit will conduct spot checks across DoP sites at random. Details of each spot check will be recorded and stored in the Information Security Management System network folder. The results of this process will be recorded in the register, including any remedial actions needed and the date that the action took place.

**Non- compliance**

In the first instance of non-compliance, the user in question will be contacted via email by the Information Governance Unit who will recommend remedial actions that must be implemented and send the user the appropriate policies for review. In the second instance of non-compliance, the user and their direct line manager will be contacted via email by the Information Governance Unit who will recommend remedial actions that must be implemented and send the user the appropriate policies for review. On the third instance of non-compliance, a meeting will be organised between the user, their line manager and the Information Governance Unit to agree an action plan and timeline for compliance. On the fourth instance of non-compliance, a meeting with the Director will be organised to discuss further remedial action.

**Further advice on secure working**

Please contact the department’s Information Governance Unit at infogov@paediatrics.ox.ac.uk if you have any questions concerning secure working.

**Document History**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Author** | **Key Changes** | **Date** | **Review By** |
| 1.0 | DOP Senior IG Manager | First published version. To be reviewed annually | 11 June 2024 | June 2025 |

1. <https://www.infosec.ox.ac.uk/create-strong-passwords> [↑](#footnote-ref-1)
2. To lock a Windows machine, hold down Windows key and press “L” or select the “start” button, select your Windows account profile picture icon and choose “lock screen”. For Macs, click on the Apple icon and then select “lock screen”. [↑](#footnote-ref-2)