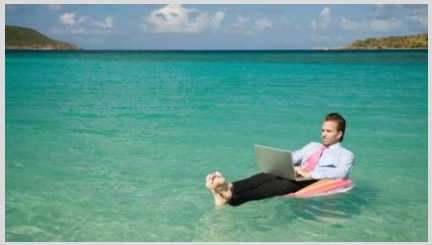
NUFFIELD DEPARTMENT OF
PRIMARY CARE
HEALTH SCIENCES

UNIVERSITY OF
OXFORD

Information Governance

Requirements for Safe Remote Working

Spring/Summer 2020



Contents:

1. BYOD Requirements for safe remote working
2. Tips for all Remote Users
3. Reporting breaches and security incidents
4. More resources

BYOD Requirements for remote working (1 of 2)

ENCRYTION: BYOD Users should encrypt their local disk where possible, using Microsoft Bitlocker for Windows and Filevault for Mac.

ANTIVIRUS: BYOD Users must deploy antivirus protection, such as Sophos, which means that the antivirus software is active, routine scanning occurs and that the device is scanned and does not contain viruses before initially accessing Department applications remotely.

COPYING/OPENING DEPARTMENT DATA: BYOD Users agree to *always* refrain from copying Department data to any BYOD from a Department network shared drive and opening such files directly from their BYODs.

BYOD Requirements for remote working (2 of 2)

PASSWORD PROTECTION: BYOD Users agree to deploy password protection on the PC, laptop or BYOD other device.

EXCLUSIVE USE: BYOD Users agree that the PC, laptop or other BYOD device on which they intend to work remotely is used exclusively by the User and his/her password is not shared with anyone else.

LICENSE RESTRICTIONS: Some software cannot be installed on User BYODs due to license restrictions, such as for STATA, Q-Research, etc. Users are advised to consult with their line managers to confirm the extent to which this may apply.

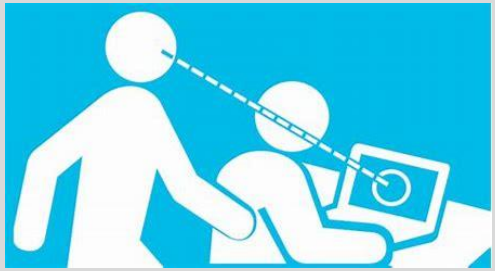
Tips for all Remote Users (1 of 2)

Refrain from the following:

- ✓ Leaving any equipment and paper information unattended at home or any other location where a reasonable level of security is not available;
- ✓ Sharing any equipment and paper information with partners, family members or others not authorised to use it; and
- ✓ Disposing any paper information in a manner that is not secure.

When working in public:

- ✓ Confirm that the User's monitor cannot be viewed by others, such as by sitting with your back to a wall (a monitor screen is not required)



Tips for all Remote Users (2 of 2)

- Use **OneDrive for Business** to remotely access any data classified as Confidential or Internal (refer to this link for more information:

  https://help.it.ox.ac.uk/nexus365/onedrive-business-usage).

  ✓ Never access data classified as **Confidential** through the University's NetStorage service and these other available options: Dropbox, Google Drive and Amazon Cloud Drive.

- Confirm that you have the means to contact the Department for advice and support in the event of the loss of all IT equipment.

  ✓ For instance, access to an alternative telephone and a list of the relevant telephone numbers.

NUFFIELD DEPARTMENT OF
PRIMARY CARE
HEALTH SCIENCES

UNIVERSITY OF
OXFORD

Reporting Incidents

An "**Incident**" is any event that poses or could poses risk to the security, integrity or confidentiality of Department information. Report all actual or suspected breaches and security Incidents.

- ✓ Report **breaches** , such as the aaccidental disclosure of information to an unauthorised individual, to: data.breach@admin.ox.ac.uk w/copy to the Department IGM (datasecurity@phc.ox.ac.uk.)

- ✓ Report **security Incidents**, (e.g. unauthorised access by sharing one's credentials with another to give him/her system access) to oxcert@infosec.ox.ac.uk w/copy to the Department IGM (datasecurity@phc.ox.ac.uk.)

Please do not delay the reporting of any breach or incident by first attempting to gather more information and/or referring it initially elsewhere within the Department.

Refer to any of these resources:

University BYOD policy:
https://help.it.ox.ac.uk/security/endpoint/byod-policy

Department Mobile and Remote Working (PHC_POL_IG106_v4):
https://ig.phc.ox.ac.uk/prisms-ig/accounts/login/

VPN and Encryption – FAQs:
https://help.it.ox.ac.uk/network/vpn/faq/index
https://help.it.ox.ac.uk/network/remote/index
https://www.medsci.ox.ac.uk/divisional-services/support-services-1/information-technology/your-computer/encryption/encryption-faqs

Guidance on breaches and security incidents:
https://compliance.admin.ox.ac.uk/staff-guidance-on-data-breaches
https://www.infosec.ox.ac.uk/report-incident