

DATA PROTECTION WHILE WORKING FROM HOME

CONTENTS

General data protection and information handling	2
Attending College meetings from home	2
Microsoft Teams	2
Chorus	2
Zoom and other Cloud applications	2
Hosting a Zoom meeting	2
Use of your borrowed work computer or mobile phone	3
Use of credentials	3
Working on documents	3
Printing to your home printer	3
Use of your personal computer or device	4
Use of credentials	4
Working on documents	4
Printing to your home printer	4
Managing printed information.....	4
Confidentiality	4
Help.....	5
Version control	5

DATA PROTECTION WHILE WORKING FROM HOME

GENERAL DATA PROTECTION AND INFORMATION HANDLING

College information generated, collected and/or processed by the College is managed according to the College records of processing activities and policies available at <https://www.new.ox.ac.uk/privacy-policy> but in more detail within the College data asset register on the College Data Protection shared drive. Please ask your head of department for any clarification around how information is managed within the College. You must work within the College policies even when working from home.

This document explains how you should work from home using remote working facilities to process College information, in line with College policies.

ATTENDING COLLEGE MEETINGS FROM HOME

MICROSOFT TEAMS

Microsoft Teams (<https://portal.office.com>) is part of the Nexus365 service and is the University's approved service for video conferencing and remote teaching. Teams is also a tool to facilitate flexible working and collaboration from anywhere.

CHORUS

The University Chorus teleconferencing service (<https://help.it.ox.ac.uk/chorus/teleconferencing>) is the University's approved service for telephone conferencing.

ZOOM AND OTHER CLOUD APPLICATIONS

The University has completed a third-party security assessment (TPSA) for use of the Zoom cloud service during the Covid-19 lockdown period. <https://infosec.ox.ac.uk/article/guidelines-for-using-zoom>. This is approved for certain types of University data/use but has not been assessed for College use. Zoom is to be used where Teams is not deemed possible.

Until the College has performed a TPSA and performed a data protection impact assessment for College processes users can assume that the University guidelines apply but that following University information classifications map to College classifications:

- "Internal" relates to "Protected data" , and
- "Confidential" relates to "Highly Protected data".

HOSTING A ZOOM MEETING

1. Register with the College DPC (dataprotection@new.ox.ac.uk) when creating an account using a College email address.
2. Read the University guidance at <https://infosec.ox.ac.uk/article/guidelines-for-using-zoom> and apply the data classifications in the section above to the type of information you will be sharing while in the meeting.
3. Refer to the guidance at <https://zoom.us/docs/doc/Securing%20Your%20Zoom%20Meetings.pdf>
4. Please also make sure that all participants of College-setup Zoom meetings accept the following notice:

We have chosen to use Zoom for certain types of meeting because we believe that it provides the best experience in the unusual circumstances that the world is in, due to Covid-19.

DATA PROTECTION WHILE WORKING FROM HOME

As a College we are both bound by and committed to our Data Protection responsibilities. Please find our data protection statement and policies at <https://www.new.ox.ac.uk/privacy-policy>. Please read the Zoom privacy policy at <https://zoom.us/privacy>, in particular the sections that mention “You” or “user” or “participant”. Information that they collect from participants is detailed under the section “Data that our system collects from you”.

Zoom provides some features that we will not be using because they are not necessary:

- Zoom provides the ability to record meetings. We will not record meetings that are hosted by College Members.
- Zoom provides an attention tracking feature. We will not enable the attention tracking feature of the application in meetings hosted by College Members.
- Zoom provides the ability to transfer files between meeting participants. We will not use this feature in meetings hosted by College Members

The information that we collect about you will be processed under our privacy policies located at <https://www.new.ox.ac.uk/privacy-policy>.

Please acknowledge by return email to me as the meeting “host” and on behalf of [College] that you have read the privacy policy and are happy to take part in meetings with us. If you are not happy to do this then we can find alternative means for meeting with you.

USE OF YOUR BORROWED WORK COMPUTER OR MOBILE PHONE

Since this a College-owned device you must not allow anyone who is not a member of staff at New College to use it. When you are not at your computer ensure it is locked and only you know the password.

USE OF CREDENTIALS

You must not share your credentials with anyone.

WORKING ON DOCUMENTS

You can use these devices to temporarily store work documents while you work on them. If you wish to transfer documents between your work and work at home computer you can use either email or the more preferred method of Nexus 365 OneDrive for temporary transfer.

PRINTING TO YOUR HOME PRINTER

If you need to print to your home printer, please ask your line manager for approval, who will then make a request to the IT department. Please be aware that only home printers connected to the home working computer via usb cable will work via remote desktop; a home network printer will be prevented by the University VPN connection. However, since this is a home working computer provided by the College you can transfer documents via email or Nexus365 and close down the VPN connection if wanting to print to a home-networked printer.

A member of the IT team can help install a home printer.

PLEASE READ THE SECTION CALLED “Managing printed information”.

DATA PROTECTION WHILE WORKING FROM HOME

USE OF YOUR PERSONAL COMPUTER OR DEVICE

Only use the remote desktop application for connecting to your work computer. When you are not at your computer ensure it is locked and only you know the password to the account that you are using for accessing the college network.

USE OF CREDENTIALS

Make sure that any credentials that you use that relate to work are not remembered. Create a separate username and password (not in common with any that you use at work) on the device for you to use.

WORKING ON DOCUMENTS

Do not download documents to your personal computer for working on. Only use your remote desktop.

PRINTING TO YOUR HOME PRINTER

If you need to print to your home printer, please ask your line manager for approval, who will then make a request to the IT department. Please be aware that only home printer connected to the home working computer via usb cable will work via remote desktop; a home network printer will be prevented by the University VPN connection.

PLEASE READ THE SECTION CALLED “Managing printed information”.

MANAGING PRINTED INFORMATION

Keep any printed material that is not deemed “public” information according to the College information handling rules (<https://www.new.ox.ac.uk/privacy-policy>) away from other members of your household

Find a safe way to dispose of the printed information. If you cannot dispose of it in a confidential manner then store it ready for taking into College for disposal. Printer material must not be placed in curb side recycling containers.

CONFIDENTIALITY

Ensure the confidentiality of meetings whether they be over phone or video conference. While working from home you may be overheard by neighbours, other family members or even your internet connected devices.

Regulators from both the US and Europe examined the security around SIRI and Alexa type devices. The reports sparked concerns related to the same, proving that SIRI and Alexa violate users' rights, in cases where devices begin recording unintentionally or without the users' knowledge. As a business, we take precautions to prove understanding and compliance with our legal obligations, and strive to adhere to high standards of privacy. Therefore, we ask you to switch off/deactivate SIRI and Alexa services during work times (where these devices are in close proximity to your work area) in order to mitigate any of the above privacy risks.

College email is available through via a browser by visiting www.office.com . You do not need a VPN to access this portal, where you have access to the full suite of office365 products.

All college related business via email must come from your college email address. You must not forward your college email to any personal email system. Further information can be found at:

<https://www.new.ox.ac.uk/sites/default/files/2019-12/New%20College%20Data%20Protection%20Policy%20v1.16.1.pdf>

DATA PROTECTION WHILE WORKING FROM HOME

HELP

Please email helpdesk@new.ox.ac.uk or seek advice from dataprotection@new.ox.ac.uk if you have any questions.

Version control

Version	Date changed	Notes
1.0	15/04/2020	Version 1.0 published