Encryption of Sensitive Data
It is essential that you observe the regulations relating to handling sensitive data that is subject to the Data Protection Act. MRC policy (which the WIMM adheres to) requires that mobile devices storing sensitive data be encrypted and password protected, this includes personally-owned systems which may be storing this data. If it is not possible to encrypt the device do not store sensitive data on it.

Macintoshes have built-in encryption software, FileVault, see:

https://support.apple.com/en-gb/HT204837

PCs running Microsoft Windows have BitLocker for encryption:

http://www.windowscentral.com/how-use-bitlocker-encryption-windows-10

The University has provided Youtube videos covering encryption of Microsoft Word, pdfs and file folders, see:

https://www.youtube.com/channel/UC4FTuOgYsOYOGAbpfBZ_7iw

If you email sensitive data to a recipient ensure the data is encrypted and that you have checked the email address of the recipient prior to sending the email.

Keeping Software Up-to-Date
Install security patches and Updates for the operating system and applications. Where possible configure your system to update the operating system and your applications automatically. Do not run outdated software – it is susceptible to malicious compromises.

Viruses & Malware
Systems running Microsoft Windows & Apple Macintoshes are vulnerable to viruses and malware attacks.

First line defence is to install an anti-virus program and **ensure it updates**.

The University has a site license for the Sophos anti-virus software which can be installed on both Microsoft Windows and Apple Macintosh systems, see:

https://www.ox.ac.uk/students/life/it/secure?wssl=1

Protecting your computer from viruses and other malware:

https://www.infosec.ox.ac.uk/protect-devices

Hardcopy
Keep all hard copy of confidential data in a locked location. Shred confidential documents rather than using recycling/rubbish bins. Delete/destroy copies once they are no longer needed and have been kept for the legal amount of time required
(there may be funder specific regulations, or more general processes).

MRC Weatherall Institute of Molecular Medicine

UKRI Medical Research Council

University of Oxford

IT Security Informat for New Starters

May 2022

Welcome!

As a new starter in the MRC Weatherall Institute of Molecular Medicine **(WIMM)** it is vital that you recognise the importance of Information Security. It is essential that you take measures to protect information of a confidential or sensitive nature.

It is mandatory for all WIMM staff to complete the University's online security Training Awareness Module:

https://infosec.ox.ac.uk/module

MRC Security Policy

The WIMM is a MRC funded institution and as well as it being a requirement that you adhere to the University of Oxford Information Security Policy the same is also true for the MRC Security Policy (unsurprisingly there are many areas of overlap between both policies) details of which can be found at:

https://www.mrc.ac.uk/documents/pdf/mrc-information-security-policy/

Regulations and Policies relating to Computer Use and Information Security

The following web page lists the University's Regulations and Policies relating to the use of computer technologies. It is essential that you familiarize yourself with these policies.

http://www.admin.ox.ac.uk/statutes/regulations/196-052.shtml

WIMM Security Policy

https://www.imm.ox.ac.uk/internal/it/computer-security/information-security-policy

University Information Security Policy & Guidance

https://infosec.ox.ac.uk/sites/default/files/Information%20Security%20Policy.pdf

https://www.infosec.ox.ac.uk/guidance-policy

Software Usage

https://help.it.ox.ac.uk/sls/useterms

lists software products available to members of the University and the licensing agreements associated with use of this software.

UK Legislation

Use of software products are also covered by UK Copyright legislation:

https://www.copyrightservice.co.uk/copyright/p01_uk_copyright_law

This legislation also protects video and audio material that is subject to copyright; breach of copyright law will result in disciplinary action. Do not install pirated software.

The Data Protection Act covers procedures in handling personal and/or sensitive data:

https://www.gov.uk/data-protection/the-data-protection-act

Guidelines for Safer Working Practices

The following is a brief outline of working practices that can be adopted to reduce compromise of data and systems. This cannot be considered comprehensive.

Use STRONG Passwords

https://www.infosec.ox.ac.uk/strong-passwords

for information on password security. Use a password manager to store passwords, e.g. KeePass.

Use a screen saver that prompts for your password if you leave your computer unattended.

Use VPN with WiFi

Using the Oxford University VPN with WiFi will add an additional layer of security to your WiFi connection. Remember that when using the Oxford VPN you will effectively be on the University of Oxford network and will be unable to print to a printer on your home network until you disconnect from the Oxford VPN.

Details of the University of Oxford VPN can be found at:

http://help.it.ox.ac.uk/network/vpn/index

Email

Do not email files containing confidential material. Use the University OxFile and Sharepoint services:

https://oxfile.ox.ac.uk

https://help.it.ox.ac.uk/nexus/sharepoint/index

Email Phishing

Learn to recognise phishing emails:

https://help.it.ox.ac.uk/email/phishing/index