Self-managed laptop and desktop devices policy
Version 2.4, December 2017

SCOPE AND REQUIREMENTS

The use of self-managed laptop and desktop devices – whether personal or University owned - is permitted for all Blavatnik School of Government data, other than those listed exceptions, provided that laptops and desktops, and their usage meet the following requirements:

- Use a vendor-supported operating system, such as Windows 10 or macOS High Sierra
- Apply operating system and application updates automatically
- Use different accounts for different users
- Use passwords that are at least 12 characters long
- Install anti-virus software, e.g. Sophos, and scan your machine regularly
- Use a modern web-browser, e.g. Chrome, Firefox, Internet Explorer, Edge or Safari
- Use only trusted USB devices
- Only download software from reputable sources and never use pirated software
- Enable the device's personal firewall
- Configure to lock after a sustained period of inactivity, e.g. 10 minutes
- Backup University data, e.g. using the University's HFS backup system
- Encrypt using technology such as Bitlocker for Windows or FileVault for MacOS; note that Windows Home does not support BitLocker and must not be used unless an equivalent encryption technology is in place
- Disable Macros by default on all Microsoft Office software
- Securely wipe via use of reputable tools prior to re-use

RESPONSIBILITY

The Head of ICT is responsible for:

- The secure use of self-managed laptop and desktop devices at BSG
- Authorising devices that can be used within their section
- Communicating this directive to all users
- Ensuring that all users are appropriately trained to meet these requirements
- Identifying, documenting and communicating any exceptions

Users are responsible for:

- Keeping self-managed laptop and desktop devices configured as per the requirements in this document
- Informing the BSG ICT team and their line manger if devices are lost or stolen
- Reporting devices infected with malware to the BSG ICT team.

EXCEPTIONS

The following activities are not authorised for use on self-managed laptop and desktop devices. If use of self-managed devices is required specific authorisation must be sought from the Head of Section:

Sensitive or confidential information, including HR and Finance data.

The University of Oxford's Information Security Team provide the tools, guidance and support for divisions, departments and colleges to implement effective local arrangements and adequately manage information security risk. We also monitor networks and systems to prevent and respond to external attacks. For more advice on securing your devices, systems and data see our website at www.infosec.ox.ac.uk

Self-managed laptop and desktop devices policy
Version 2.4, December 2017

HOW TO

Here's what you need to do to meet the requirements on Apple Mac and Windows 10 devices:

Apply Operating System Updates Automatically

- System Preferences > App Store > Tick "Automatically check for updates"; "Download newly available updates in the background"; "Install app updates"; and "Install system data files and security updates"
- Settings > Update & Security > Advanced options > Pause Updates is set to "Off"

Use different accounts for different users

- System Preferences > Users & Groups
- Settings > Accounts > Family & other people

Set secure passwords

- System Preferences > Users & Groups > Change Password
- Settings > Accounts > Sign-in options > Password > Change

Enable device's personal firewall

- System Preferences > Security & Privacy > Firewall > Turn On Firewall
- Start > Windows Defender Security Centre > Firewall & network protection > Domain network AND Private network AND Public network > Windows Defender Firewall is set to "On"

Configure to lock after sustained period of inactivity

- System Preferences > Security & Privacy > General > Select "Require password immediately after sleep or screen saver begins AND System Preferences > Desktop & Screen Saver > Screen Saver > Select "Start after 10 Minutes"
- Settings > Personalisation > Lock screen > Screen saver settings > Screen Saver is not set to "(None)" AND "On resume, display log-on-screen" is ticked AND changes are applied

Encrypt the device (Apple Mac and Windows 10 Professional/Enterprise only)

- System Preferences > Security & Privacy > FileVault > Turn On FileVault
- Start > type "encryption" > Manage BitLocker > Turn on BitLocker > follow instructions

Disable Macros by default

- MS_OFFICE_APPLICATION > Preferences > Security & Privacy > Disable all macros with notification
- MS_OFFICE_APPLICATION > File > Options > Trust Centre > Trust Centre Settings > Macro Settings > Disable all macros with notification

Use vendor supported operating systems

- The most recent operating systems will still be receiving security updates but some older ones do not. Microsoft's security lifecycle has guidelines on the support it provides to its operating systems. Officially, Apple only supports the latest version of its operating system. In practice Apple OS updates should be applied within 3 months or release with timings dependent on support for key applications.

The University of Oxford's Information Security Team provide the tools, guidance and support for divisions, departments and colleges to implement effective local arrangements and adequately manage information security risk. We also monitor networks and systems to prevent and respond to external attacks. For more advice on securing your devices, systems and data see our website at www.infosec.ox.ac.uk

Install and configure anti-virus software

- All staff and students are automatically entitled to a free copy of Sophos Anti-Virus, for as long as you're here. It's available for PC, Mac and Linux, and you can find a copy and instructions on the IT Services website.

Use a modern web-browser

- We recommend Chrome, Firefox, Internet Explorer, Safari or Edge. Make sure they're configured to update automatically.

Use trusted USB devices

- Don't share USB storage devices with colleagues and don't plug untrusted USB devices into your machines. Use a dedicated, encrypted USB device (can be purchased from the IT Services online shop).

Reputable Apps

- Use Apps from the Apple or Microsoft stores and legitimate copies of the software from established sources such as Adobe, Mozilla or the Free Software Foundation. Never install pirated software and get advice from your IT department if you have any concerns.

Backup Data

- Make use of the University's HFS system which is available for staff and postgrads. Contact your local IT support for more details on departmental backups. If you are using your own cloud or USB devices make sure you encrypt the data/device and ensure the use of cloud services is approved by your line manager.

Securely wipe before re-use

- Reformat the disk using a data destruction tool such as DBAN or Apple's Disk Utility.