Somerville College
Policies and guidance
Staff and academics

Bring Your Own Device (BYOD)	Created: May 2023 Last updated: N/A Approved by: Author(s): Librarian and Head of IS Statutory?: No Issue version: 1 Related documents: Personal Data Breaches: policy and procedure for reporting and investigating
Policy	

Introduction

It is not unusual for college staff and academics to use their own privately-administered devices (synonymously referred to as 'bring-your-own devices', or BYOD) when carrying out college business. While it is college policy now to provide laptops instead of desktops to enable remote working for staff, many staff and academics work from their own devices where it is more convenient or where there is no option of a college-provided device. These devices are administered by the device owner, and are not administered by the college or a university department.

This policy outlines the expectations of the college in relation to the use of privately-administered (BYOD) devices when carrying out college business. It is the college's aim to ensure all staff and academics comply with data protection legislation and college policies on data handling.

The policy also provides guidance on the remote working environment to ensure all work is undertaken in a safe manner to safeguard the personal health and safety of the staff member.

The risks to the college from those who use their own devices but who do not follow this policy include:

- The loss or theft of personal data of colleagues or students if devices are accessed by those without authority, either through hacking, poorly protected devices or the sharing of devices; and the possible resulting penalties imposed from external bodies for a breach of data protection legislation.
- Increased vulnerability of the college network to malware, viruses or hacking, and the associated potential loss of data and threat to business continuity.

Definitions

Privately-administered device: any device where the staff member as owner of the device is directly responsible for its maintenance, operating system updates, installation of anti-virus and other anti-malware software, and general security features. Devices issued by university departments to academic staff are considered privately-administered and BYOD for the purpose of this policy, as practices within departments about the extent they administer devices provided to their staff vary widely, and the college cannot be certain that the devices meet the requirements outlined in this policy.

Mobile device: any device which can store data and can be easily carried around while in use, for example, laptops, mobile phones, tablets.

Bring Your Own Device: any device on which college business is undertaken which is not provided by the college (see *Privately-administered devices* above).

Removable media: any device on which can be stored data and which has to be connected to a computer to be accessed.

Remote working: any work for the college performed outside the college site, which requires access to Somerville College's data, on any college or university network, system or database, including email and/or Teams.

Safe condition: physically intact equipment (including plugs and flexes), a screen which does not flicker, arranged to avoid or minimise trip hazards for the staff member and other users of the space.

Working safely: a physical environment which meets DSE requirements, with equipment in a safe condition.

Working securely: adherence to college policies and data handling practices to ensure the security of any college data and the device(s) on which it is processed, whether personal or college-owned.

Data breach: a security incident that has affected the confidentiality, integrity or availability of personal data resulting from when data is accidentally lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

Compliance with Data Protection Legislation

Large amounts of personal data are processed within Somerville College. As data controller, the college is responsible for ensuring the physical and digital security of this data. Data security in college also contributes to the security of data processed in the University more widely. The University of Oxford is a major target for hackers, seeking to penetrate systems, steal or corrupt data and hold it to ransom. A data security breach at college level could have repercussions elsewhere in the University.

For this reason, any staff or academics using their privately-administered (BYOD) devices must adhere to college policies to ensure the security of college systems and the data stored on them. By signing their contract all members of the college are agreeing to adhere to this policy.

1) **All Devices**

- Access to any device must be restricted by a password, PIN or biometric security such as fingerprint and facial recognition.
- No one except the staff member should have access to work documents or college data. The employee should log out of all accounts before allowing another person to use a shared device.
- All devices should be encrypted, and USB drives and other external hard drives must be encrypted.
- All devices must have the latest operating system available to them.

- All devices should have enabled security software such as Windows Defender or Sophos. This software should be kept up-to-date. (Please note Sophos is available from the University.)
- Apps should be downloaded only from official sites or the Apple or Android app stores.

2) **Mobile devices**

- Mobile devices and removable media devices and mobile phones must be kept secure at all times.
- Ideally mobile devices should have location tracking software installed, and the ability to wipe the device remotely.

3) **Network and internet access**

- Open, unsecured WiFi sources in cafes or libraries should not be used for college business.
- Secure network access should be used where possible as provided by the college, including the VPN and remote desktop access.

4) **Removable media, such as USB and external hard drives**

- Removable media must be encrypted before use.
- Any employee who intends to store college data on removable media must be authorised to do so by the Head of Department or Senior Manager (as appropriate).
- Only data that is authorised and is necessary to be transferred should be saved to removable media devices.
- Sensitive data (e.g. special category data such as data relating to physical/mental health, financial information, lists of donors, students home addresses) should not normally be saved to removable media. Specific rules regarding the use of data in the alumni database (or any other database in use at the college) must be adhered to at all times.
- Removable media should not be the only place where data obtained or used for work purposes is held. Copies of the data should be available on and backed up to the college servers.
- College data should not be kept on removable storage media for longer than necessary

Reporting of data breaches

- It is the duty and responsibility of all employees to report immediately any actual or suspected data breaches to their manager or head of department. The procedure detailed in the document *Personal Data Breaches: Policy and procedure for reporting and investigating* should be followed.
- All losses of devices, unauthorised access to data, corruption of data, or any other incident which leads to an actual or potential data breach as defined above should be reported.

Damaged, faulty or end-of-life devices and media

- Damaged or faulty devices or media must not be used.
- All data should be removed from obsolete or faulty devices before being disposed of.

Compliance with DSE legislation

Employees should ensure that the computing equipment they use at home in order to carry out college business is maintained in a safe condition.

Employees are required to carry out their own DSE assessment as employees are personally responsible for:

- Arranging their equipment and workstations in accordance with current recommendations. The DSE Assessor can provide guidance on the appropriate seating position.
- Completing a DSE assessment form on their home workstation
- Arranging a timely repair if their computer screen flickers or their equipment, including the flexes and plugs, becomes physically damaged.
- Reporting, without delay, to their manager any discomfort e.g. tingling sensations or pains in their hands, forearms or necks, thought to be associated with the use of the workstation. If symptoms are identified, the manager must arrange with the Human Resources Manager for the employee to attend an assessment with the University Occupational Health Service. Please note that if working from home is not required as part of the role, replacement equipment will not be provided at the expense of the college. Instead, employees who do not have a suitable working space at home will be asked to work in college. Exceptions will be made for those for whom working at home is a requirement.
- Taking regular breaks away from the workstation

Employees must ensure that their home insurance policy includes cover for use of personal equipment for work purposes as the college will not be held liable for loss or damage to personal equipment used for work purposes.

IT support for policy compliance

IT provide technical support for devices provided by the college, and are not responsible for technical support for personal devices. An exception may be made where the personal device is the only device available for college business and the technical support is required specifically for the purpose of college business.

IT can provide advice on best practice in the support of securing data. They are able to recommend practices and software which will enable users to comply with the guidance within this policy, including advice on encrypting devices or installing anti-virus software, as well as general guidance on how to connect devices to networks and the internet.