UNIVERSITY OF SUSSEX

IT Services

BRING YOUR OWN DEVICE POLICY

1. OVERVIEW AND PURPOSE

1.1. This document sets out the University's policy on the use of devices that are not owned or managed by the University to access University information and/or information technology services (commonly referred to as Bring your Own Device - BYOD) as part of the suite of Information Security policies.

1.2. Whilst the University recognises the benefits of allowing BYOD for work and study, such devices pose a security risk if not adequately protected.

1.3. The objective of this policy is to mitigate risks to the confidentiality, integrity and availability of University data, information and information technology services arising from BYOD.

1.4. This policy sets out the safeguards necessary to allow BYODs to access University information technology services without imposing unrealistic conditions on how such devices are configured.

2. SCOPE

2.1. This BYOD policy refers to any networked computing device with the capability to access the University's networked resources or services and that is not owned or managed by the University including, but not restricted to, phones, tablet computers, laptops, desktop computers, servers and gaming consoles. These are referred to as personal devices or simply as devices hereafter.

2.2. University information technology services shall be taken to mean any digital information or service provided or procured by the University and accessible through the University network or over the Internet. Information shall be taken to mean information and data processed by the University.

2.3. This policy applies to all users including staff, students, associates, visitors and guests of the University using their device(s) to access University information technology services.

2.3.1. Visitors and guests normally only have access to University information technology services in the form of Eduroam access granted by their home institution. Eduroam terms of use stipulate that such users will be bound by their home institutions policy and the policy of any other institution at which they use Eduroam. Such users will be able to use the campus Eduroam network to access the internet, but no other University services.

2.4. If a device does not have capability to connect to University information technology services, there is no obligation on the University to modify services or provide support in connection.

2.5. This policy applies at all times.

3. RESPONSIBILITIES

3.1. Information Governance Committee (IGC)

3.1.1. Ensuring that the necessary processes and systems are in place to support this policy.

3.1.2. Ensuring that this policy is regularly reviewed and remains fit for purpose.

3.2. Senior Information Risk Officer (SIRO)

3.2.1. Ensuring that this policy aligns with the University's risk appetite.

3.2.2. Ensuring that information risks associated with the use of personal devices are appropriately identified and managed.

3.3. Director of IT Services

3.3.1. Ensuring that this policy and security of information in the context of BYOD aligns with and supports the University's agreed strategic framework for information technology services.

3.3.2. Ensuring that adequate technical advice and guidance is made available to all including staff, students, associates, visitors and guests of the University using personal device(s) to access University information technology services.

3.4. **IT Services**

3.4.1. Providing limited advice and support for BYOD. The primary objective is to ensure that individual requirements can be met while ensuring that the confidentiality, integrity and availability of University information and information technology services is not compromised.

3.5. **Data Protection Officer (DPO)**

3.5.1. Ensuring that data protection risks associated with the use of personal devices are appropriately identified and managed.

3.5.2. Advising on the development and maintenance of the data protection aspects of this policy.

3.6. **Heads of Schools, Directors of Professional Services Divisions**

3.6.1. Ensuring compliance with this policy in their areas.

3.6.2. Ensuring that those acting under this policy (for whom they have management or contractual responsibility) are appropriately trained and made aware of their obligations.

3.7. **Anyone using personal devices to access University Services**

3.7.1. Complying with this policy.

3.7.2. Reporting any personal data breach immediately to the Data Protection Officer.

3.7.3. Reporting any information security incidents or risks to the IT Service Desk immediately.

4. POLICY

4.1. Users must ensure that they use their devices in compliance with the Information Security Policies including the IT Regulations and IT Remote Working Policy and Guidance.

4.2. The contents of University information technology services and University information remain University property.

4.3 All materials, data, communications and information, including but not limited to, e-mail messages, voicemail, recorded telephone conversations, SMS and instant messages, and social media postings, produced or carried out as part of work for the University or on its behalf remains the property of the University, regardless of who owns the device, unless agreed in writing otherwise. All teaching materials provided to students remain the property of the University or the relevant copyright holder.

4.4. As far as possible University data and information should not be stored on personal devices (see Information Classification and Handling Policy and associated guidance). If a personal device is used to access sensitive or protected information from University information technology services, the device connection to University information services must be secure. If sensitive or protected information is accessed in such a way that the information is stored on the device, the storage location must be encrypted (see Cryptography Policy). If a BYOD user is in doubt as to whether this is the case, they should assume that information will be stored on the device and act accordingly. IT Services can give guidance on this.

4.5. University information copied to or stored on personal devices may be subject to the Freedom of Information Act and Data Subject Access Rights under the Data Protection Act 2018 and must be provided to the Information Management department on request.

4.6 The University may utilise Mobile Application Management (MAM) solutions which help to protect and secure University information whilst enabling users to utilise their devices without compromising security. MAM policies are not deployed directly to the device. Instead, the policy is associated with the application that is to be managed. When the application is deployed and installed on devices, the settings that have been specified will take effect. MAM allows the University to remove all University protected data from any MAM enabled applications.

4.7. **Devices**

4.7.1. Users who require access via personal devices must ensure their devices are sufficiently protected against attack. Operating systems must have the latest patches installed, anti-virus active and current, and a personal firewall should also be active and kept up to date. If a BYOD user is in doubt as to whether this is the case the IT Services helpdesk can give guidance.

4.7.2. The transfer of data to USB memory sticks, other removable media (e.g. CDs/DVDs/portable hard drives) and other mobile media devices (e.g. smartphones, laptops) is discouraged. Files should be stored on University's provided services such as Box or OneDrive and not on BYODs or removable media. If the use of removable media or mobile media devices is the only practicable solution, then encryption may be required. Please refer to the Information Classification and Handling and Cryptography policies for further information.

4.8. **Security/User Responsibilities**

4.8.1. In order to prevent unauthorised access devices must be secured by a PIN, password, fingerprint or other comparable method.

4.8.2. The University's preference is that the device is not shared with others. If the device is shared with others (for example a family owned laptop or desktop computer), a user account that can only be accessed by the University user must be used for any University business.

4.8.3. Users must take suitable precautions to protect the device and information being processed, including:

- Adherence to clear desk and clear screen practice
- Ensuring screens/sessions are locked or terminated when not in use
- Where possible, not leaving the device unattended
- Not permitting someone else to use the device whilst the University user session is unlocked

4.8.4. Users must follow the password policy, not divulge passwords to anybody and leave nothing on display that may contain information such as login names and passwords. Users should also avoid options such as “remember my password” or “stay logged in” on the device. The use of reputable password managers is acceptable.

4.8.5. Be mindful of information security if using devices during journeys in public environments to avoid the risk of theft of the device or unauthorised disclosure of University information by a third party observing the screen or keystrokes.

4.8.6. Users must take care when connecting to public networks, such as those provided by cafes and hotels, where there is an increased risk of interception. Appropriate care would be using a VPN to connect to University information technology services other than email, and ensuring an encrypted connection is used for email if not using VPN.

4.8.7. Users must report to IT Service Desk or on-site campus Security team any lost or stolen devices as soon as possible of becoming aware the device is missing, at least within 24 hours.

4.8.8. Notify any suspected breaches or weaknesses to the IT Service Desk.

4.8.9. Rooted (Android) and Jailbroken (iOS) devices are strictly forbidden from accessing the network.

4.8.10. No direct access to the Card Holder Data (CHD) environment is permitted from personally owned devices.

4.8.11. MAM-protected University information on the users’ device will be remotely wiped if:

- The device is lost or stolen
- The device is no longer used, or access is no longer required
- On termination of employment / study / assignment (by either party)
- The device has been offline for more than 90 days
- A data or policy breach is detected
- A virus or similar threat to the security of the University’s information technology services is detected.

4.8.12. Use of any non-University device is at the users' risk. In the unlikely event that a users' own data on the device is affected or lost, the University will not be held responsible or liable for any damages or compensation.

4.8.13. Remote connectivity issues can be supported by the IT Service Desk provided the devices meet the above conditions, however for operating system or hardware related issues the user should contact the device manufacturer.

4.9. **Software Licensing**

4.9.1. All devices must use correctly licensed software. For personal devices it is the users' obligation to ensure that all software is legal and paid for where necessary.

4.9.2. The University is responsible for any client access licenses that maybe required when connecting personal devices University information technology services, which may include, MAM, VPN software, etc.

4.9.3. Only software approved by IT Services may be used with the institution's IT systems.

4.10. **Risks / Liabilities / Disclaimers**

4.10.1. People use their own devices at their own cost and should have an adequate data plan. The University will not reimburse any charges incurred by the user.

4.10.2. It is device users' responsibility to ensure that they have suitable hardware and software for accessing University information technology services, the University will not be held accountable for any non-prior agreed hardware or software purchases.

4.10.3. Whilst IT Service Desk will take every precaution to prevent the user's own data from being lost in the event it must remote wipe a device, it is the users' responsibility to take additional precautions such as backing up their own data from their device.

4.10.4. The user assumes full liability for risks including, but not limited to, the partial or complete loss of University and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.

4.10.5. The user is liable for all costs associated with their personal device.

4.10.6. People use personal devices at their own risk and the University is not liable for any costs associated with the loss or damage of devices.

4.10.7. Personal devices are not covered under the University's insurance.

4.11. **Breach of this policy**

4.11.1. Where there is a deliberate misconduct or behaviour amounting to wilful breach of this policy, or gross negligence causing a breach of the policy, the matter may be considered using the University's Disciplinary Procedure under Regulation 31.

5. LEGISLATION AND GOOD PRACTICE

5.1. The National Cyber Security Centre (NCSC) have issued guidance about Bring Your Own Device (BYOD) https://www.ncsc.gov.uk/collection/mobile-device-guidance/bring-your-own-device

5.2. The Payment Card Industry Data Security Standard has requirements regarding the storage, processing and transmission of cardholder data.
https://www.pcisecuritystandards.org/pdfs/pci_ssc_quick_guide.pdf

5.3. Cyber Essentials helps to guard against the most common cyber threats and demonstrate commitment to cyber security.
https://www.ncsc.gov.uk/cyberessentials/overview
https://iasme.co.uk/cyber-essentials/

Review / Contacts / References	
Policy title:	Bring Your Own Device Policy
Date approved:	20 October 2020
Approving body:	Information Governance Committee
Last review date:	20 June 2017
Revision history:	0.3 Issued to ISC 20/02/2015 Jerry Niman 1.0 Approved by ISC for Issue 03/03/2015 1.1 Minor Amendments
Next review date:	October 2021
Related internal policies, procedures, guidance:	Information Security Policies Information Security Policy Cryptography Policy Information Classification and Handling Policy IT Remote Working Policy Regulations for Use of Information Technology Guidance Notes on the Regulations for the Use of Information Technology (Acceptable Use) ITS Top 10 Security Tips Data Protection Payment Card Industry Data Security Standard Policy Regulations of the University
Policy owner:	IT Services
Lead contact / author:	Suzanne Elmore, Cyber Security Manager