Name of policy - Bring Your Own Device (BYOD) Policy

Version number - v1.0

Effective date - 11th June 2026

Bring Your Own Device (BYOD) Policy
Version 1.0

Policies superseded by this version

This document replaces the legacy Bring Your Own Device (BYOD) Policy of St George's, University of London, with effect from 11th of June 2026.

Summary of changes to previous version

The policy has been re-written following a review due to the merger of City, University of London and St George's, University of London. The policy has been aligned with the University's IT Acceptable Use Policy and Hardware Asset Management Policy, restructured to the University's policy template and updated to reflect current ISO 27001:2022 control requirements.

Table of contents

1 Introduction

City St George's, University of London ("the University") recognises that staff, students and other authorised users may use personally owned devices to access University information systems and data. While the University provides managed devices as the primary means of accessing its systems, the use of personal devices for University work is a practical reality, particularly in the context of remote and hybrid working, and must be governed to protect University data and infrastructure.

This policy establishes the conditions under which personally owned devices may be used to access University systems and data, defines the security requirements that must be met, and sets out the restrictions on what information may be accessed or stored on such devices. It supports the University's information security management system (ISMS) and aligns with the IT Acceptable Use Policy, the Hardware Asset Management Policy and the Data Protection Policy.

The University's position is that managed, centrally supported devices are the most secure option for accessing University information, and users are strongly encouraged to use a University-provided device wherever one is available. Personal devices are permitted as a supplementary means of access, subject to the requirements of this policy, but they are not a substitute for the managed computing environment.

Nothing in this policy restricts the use of personal devices for accessing publicly available University information, such as the University website, or for connecting to the University's guest wireless network for personal use.

2 Freedom of Speech and Academic Freedom

2.1 City St George's, University of London, regards freedom of speech and academic freedom to be fundamental to delivering its mission as the University of business, practice and the professions. Its values in this respect are set out in a code of practice on freedom of speech and academic freedom, which explains how the University will uphold, secure, and promote freedom of speech within the law: https://www.citystgeorges.ac.uk/about/governance/policies/code-of-practice-on-freedom-of-speech.

2.2 Nothing in this policy should be interpreted in any way that would be inconsistent with the code of practice and – in the event of any inconsistency – the provisions of the code will prevail.

3 Equity, Diversity and Inclusion

3.1 City St George's, University of London works to advance equity, diversity and inclusion in its activities, processes, and culture, for the whole University community, including staff, students and visitors.

3.2 The University will meet its obligations under the Equality Act 2010 in its policies and seek to eliminate discrimination on the basis of age, caring responsibilities, disability, gender identity, gender reassignment, marital status, neurodiversity, pregnancy, race, religion or belief, sex, sexual orientation, and socio-economic background.

4 Definitions

Term	Definition
Personal device (BYOD)	Any internet-connected endpoint device that is personally owned and not centrally managed or supported by the University's IT department. This includes personal laptops, desktops, tablets, smartphones and home computers.
Managed device	A device owned by the University, configured and maintained by IT, running the University's standard operating environment and subject to centrally deployed security controls.
Endpoint device	Any computing device capable of storing or accessing digital data and connecting to University networks or systems.
University data	Any information created, received, stored or processed in the course of University business, regardless of format or location.
Mobile device management (MDM)	Software used by the University to manage, monitor and enforce security policies on devices that access University systems and data.
Conditional access	Technical controls that evaluate the security posture of a device and the context of an access request before granting access to University systems.
Multi-factor authentication (MFA)	An authentication method requiring two or more verification factors to access a system.
Jailbreaking / rooting	The process of removing manufacturer-imposed restrictions on a device's operating system, which bypasses built-in security controls.

5 Policy

The University permits the use of personal devices to access University systems and data, subject to the conditions set out in this policy. The use of a personal device for University purposes is a privilege, not a right, and may be restricted or withdrawn at any time if the University considers that a device or user poses a risk to its systems, data or infrastructure.

5.1 Purpose

The purpose of this policy is to establish the University's overarching approach to cyber security and to set out the controls, responsibilities and obligations that apply across its digital estate. It provides the framework within which the University will protect its information systems, networks, devices and data from cyber threats, whether accidental or intentional.

Specifically, this policy seeks to:

- Protect the confidentiality, integrity and availability of University information systems and data from cyber threats.
- Provide a consistent and institution-wide approach to managing cyber risk following the merger of City, University of London and St George's, University of London.
- Enable the University to respond effectively to cyber security incidents and minimise the impact of any breach on its operations, reputation and the individuals whose data it holds.

This policy applies to all University systems, networks and users and must be read in conjunction with the University's Information Security Policy and all related subsidiary policies.

5.2 Scope

This policy applies to all users who access University information systems or data using a personally owned device that is not centrally managed by the University's IT department. This includes staff, students, researchers, visiting academics, contractors, consultants, and any other authorised persons.

The policy covers all types of personal endpoint devices, including but not limited to personal laptops, desktops, tablets, smartphones, and home computers.

This policy does not apply to university-owned managed devices, which are governed by the Hardware Asset Management Policy, or to the use of personal devices solely for accessing publicly available University information or the guest wireless network.

5.3 Roles and responsibilities

Effective information security relies on all users understanding and fulfilling their responsibilities. The following roles have specific duties in relation to this policy and the ISMS:

a. Senior Information Risk Owner (SIRO)

The Deputy President (Operations) acts as the SIRO and owns the overall information risk for the University. The SIRO chairs the Information Governance and Security Committee (IGSC) and is accountable for ensuring that information risks are managed effectively across the institution.

b. Chief Information Officer (CIO) and Deputy CIO

The CIO holds operational accountability for information security, supported by the Deputy CIO. Together they ensure that appropriate technical, procedural and governance measures are in place to

support the ISMS, approve security exceptions and escalate risks that exceed the University's risk appetite.

c. Information Security Manager

Maintains this policy and the ISMS, oversees the implementation of information security controls, provides expert advice, conducts risk assessments, manages the security incident response process and monitors compliance through audits, reviews and security assurance activities.

d. Data Protection Officer (DPO)

Advises on compliance with the UK GDPR and Data Protection Act 2018, assesses data protection risks, manages information rights requests and ensures that data protection considerations are integrated into information security controls and incident management.

e. Information Governance and Security Committee (IGSC)

Provides oversight, challenge and assurance for information security and governance matters, including policy approval, risk management and monitoring of compliance across the institution. The IGSC reports to the Senior Leadership Team and the Audit and Risk Committee.

f. Information Assurance Team

Responsible for advising on compliance with data protection legislation, managing the DPIA process, maintaining Records of Processing Activities and ensuring that organisational, procedural and technical controls collectively support a compliant and risk-aware environment.

g. Line managers and supervisors

Ensure that users within their teams understand and comply with information security policies, complete mandatory training and follow established procedures. Managers must notify IT promptly when staff or contractors change roles or leave the University.

h. System owners and data owners

Ensure that systems and information under their stewardship are classified correctly, protected in accordance with University standards and supported by appropriate risk assessments, DPIAs and access controls.

i. All users

All users are responsible for information security and must ensure that University systems are used in a secure and compliant manner. Users must protect their credentials, follow security guidance, complete mandatory training and report actual or suspected incidents without delay. For clarity, reporting obligations relate to specific security risks, policy breaches or unlawful activity, not the mere fact that opinions expressed may be controversial.

j. Third-party service providers

Where third parties process University data or provide technology services, they must comply with contractual requirements, applicable legislation and the University's security standards. Contract

managers must ensure appropriate due diligence, risk assessments and data-processing agreements are in place.

5.4 Principles

- Managed devices are the University's preferred and most secure method of accessing its information systems. Users who have been allocated a University device should use it for University work.
- Personal devices may be used as a supplementary means of access but must meet the minimum security requirements set out in this policy before accessing University data.
- University data accessed via personal devices remains the property of the University and is subject to the same legal, regulatory and policy obligations as data held on managed devices, including the Freedom of Information Act 2000, the Data Protection Act 2018 and UK GDPR.
- Information classified as highly confidential or restricted under the University's information classification framework must not be downloaded to or stored on personal devices. Such information should only be accessed using University-managed devices connected to trusted networks.
- The University reserves the right to restrict or remove access from any personal device that it considers to be a risk to its systems, data or infrastructure, including the right to remotely remove University data or revoke access to University services.
- Users are responsible for ensuring their personal devices meet the security requirements of this policy. The University does not provide technical support for personal devices.
- Certain roles, functions or access levels may require security measures that prevent the use of personal devices entirely. Where the nature of a role or the sensitivity of the systems or data involved means that access from personal devices would present an unacceptable risk, the University will restrict access to managed devices only. Users in such roles will be informed of this restriction and provided with appropriate University equipment.

5.5 Device security requirements

The following security requirements must be met before a personal device is used to access University systems or data:

- The device must run a supported operating system that is receiving security updates from the vendor. A device must not be used to access University data once the vendor ceases to provide security updates.
- All available security patches and operating system updates must be installed. Automatic updates should be enabled wherever possible.
- The device must be protected by a passcode, password or biometric authentication. Default or weak credentials must be changed before accessing University data.
- Anti-malware software must be installed and kept up to date on laptops and desktop computers. The operating system's built-in firewall must be enabled.
- Devices that have been jailbroken (iOS) or rooted (Android) must not be used to access University systems or data.
- Full disk encryption must be enabled on laptops and desktop computers. Mobile devices with built-in encryption (such as iOS devices with a passcode enabled) meet this requirement.
- The device must comply with the University's conditional access policies. Devices that do not meet the required security posture will be denied access automatically.
- Multi-factor authentication (MFA) is required for all remote access to University systems. Any attempt to circumvent MFA will result in access being removed and will be treated as a breach of this policy.

5.6 Data restrictions

The following restrictions apply to the handling of University data on personal devices:

- Information classified as highly confidential or restricted must not be downloaded from University systems or stored on personal devices or personal cloud storage. This includes personal data as defined under UK GDPR, commercially sensitive information and research data subject to contractual confidentiality obligations.

- University data that is classified as internal or public may be accessed via personal devices through University-approved applications and services.
- Personal devices must not be used as the sole repository for any University information. The master copy of University data must always be held on University-approved systems and storage services.
- Users must not use personal email accounts, personal cloud storage or unapproved third-party services to store, process or transmit University data.
- Users must only access University data through University-approved applications and services, such as Microsoft 365, Outlook, Teams and OneDrive for Business.

5.7 **Network restrictions**

- Personal devices must not be connected to the University's corporate wired network. This includes plugging personal devices directly into network sockets in offices, labs or teaching spaces.
- Personal devices may connect to the University's wireless network using the designated BYOD or eduroam wireless service. Access to the corporate VPN from personal devices is not permitted unless specifically authorised by IT.
- Users should avoid connecting to unknown or untrusted wireless networks when accessing University data. Where this is unavoidable, a reputable VPN service or encrypted connection should be used.

5.8 **Use and maintenance**

- Users must take care when accessing University data in public places and must be aware of the risk of shoulder surfing, eavesdropping and theft.
- Users must not share their personal device with other people for the purpose of accessing University systems or data. Where a device supports multiple user accounts, a separate account without administrative privileges should be used for University work.
- Users must keep their device's operating system, applications and security software up to date with the latest patches and updates.
- The University does not provide technical support for personal devices. Users are responsible for the configuration, maintenance and security of their own devices.

5.9 **Secure deletion and disposal**

Users must ensure that all University data, information and applications stored on a personal device are securely deleted:

- When the user's affiliation with the University ends, including at the end of employment, study or contract.
- When the user stops using the device for University purposes.
- Before selling, transferring, donating, recycling or disposing of the device.
- Where possible, the device should be fully wiped or factory reset. Any personally held backups containing University data must also be securely deleted. Guidance on secure erasure is available from the National Cyber Security Centre (NCSC).

5.10 **Loss, theft and unauthorised access**

- Users must report the loss, theft or suspected unauthorised access of a personal device that has been used to access University data immediately to the IT Service Desk and, where applicable, through the University's data breach reporting procedure. Staff must also notify their line manager.
- Users must cooperate with any investigation, which may include providing access to the device or assisting with the remote removal of University data.
- Where a device is lost or stolen, the University may remotely revoke access to University services and, where technically possible, remotely remove University data from the device.

5.11 **Mobile device management**

The University may require personal devices that access certain University services to be enrolled in the University's mobile device management (MDM) platform or to comply with conditional access policies.

Enrolment enables the University to enforce security settings, verify device compliance and, where necessary, remotely remove University data in the event of loss, theft or policy breach.

The University will not monitor the personal content of enrolled devices. MDM capabilities are limited to enforcing security policies and managing University data and applications. Users who do not wish to enrol their device in MDM may be restricted from accessing certain University services from that device.

5.12 Device registration and data processing

When a personal device is used to sign in to University services such as Microsoft 365, the device is automatically registered with the University's identity platform (Microsoft Entra ID). This registration creates a device identity that enables the University to apply conditional access policies and manage access to its services. Users should be aware that this registration occurs as part of the normal sign-in process.

As a result of device registration and any subsequent MDM enrolment, the University will hold information about the device. This may include the device name, manufacturer and model, operating system and version, device identifier, compliance status, encryption status, date of last sign-in and the identity of the registered owner. Where MDM is in use, the University may also hold information about managed applications installed on the device.

The University will not access or collect personal content from registered devices, including personal files, photographs, messages, browsing history, personal applications, or location data. The processing of device information is carried out under the University's legitimate interest in protecting its information systems and data, in accordance with Article 6(1)(f) of UK GDPR. Further information on how the University processes personal data is set out in the University's privacy notices, available on the University website.

Device records will be retained for as long as the device remains registered. Users may request the removal of their device registration through the IT Service Desk or by removing their university account from the device. When a user's affiliation with the University ends, device registrations will be reviewed and removed in accordance with the University's account lifecycle procedures.

6 Procedure

6.1 Accessing University systems from a personal device

Before using a personal device to access University systems, users must ensure their device meets the security requirements set out in section 5.4 of this policy. No prior registration or approval is required for general access via university-approved cloud services (such as Microsoft 365), provided the device meets the University's conditional access requirements.

Where access to specific systems or services requires MDM enrolment, instructions are available from the IT Service Desk and the University intranet.

6.2 Reporting security incidents

All users must report actual or suspected security incidents involving personal devices immediately to the IT Service Desk or through the University's incident-reporting channels. This includes:

Loss or theft of a personal device that has been used to access University data.

Suspected malware infection on a device used to access University systems.

Suspected unauthorised access to university data via a personal device.

Any use of a personal device to access University data contrary to this policy.

Staff must also notify their line manager. Incidents will be managed in accordance with the University's Information Security Incident Management Procedure.

6.3 Leaving the University

Before the end of their affiliation with the University, users must securely delete all University data from personal devices and any personal backups. Line managers and supervisors should remind departing

staff of this obligation as part of the offboarding process. The University reserves the right to request confirmation that data has been removed.

6.4 **Exceptions**
Exceptions to this policy must be requested in writing, supported by a business justification and risk assessment, and approved by the Information Security Manager. Approved exceptions will be time-limited, recorded in the security exceptions register and reported to IGSC.

7 Advice and guidance

7.1 **IT Service Desk:** The first point of contact for general IT queries, reporting incidents and seeking assistance with access or security-related concerns.

7.2 **Information Security Manager:** Provides specialist advice on information security controls, device security requirements, risk assessments and compliance with this policy.

7.3 **Data Protection Officer (DPO):** Offers guidance on UK GDPR and the Data Protection Act 2018, including how personal data should be handled when accessed from personal devices.

7.4 **Additional guidance:** Further information on device security, approved applications, MDM enrolment and secure deletion is available on the University intranet. The National Cyber Security Centre (NCSC) publishes guidance on securing personal devices that users may find helpful.

8 Failure to comply

8.1 **Users**
Any breach of this policy may result in the withdrawal or restriction of access to University systems, mandatory retraining or other corrective measures. Serious or repeated breaches may lead to disciplinary action under the relevant University procedures for staff or students. Contractors and third-party users may have their access terminated and may be subject to contractual remedies.

8.2 **Users**
The following are considered serious breaches of this policy:

- Downloading or storing highly confidential or restricted information on a personal device.
- Failure to report the loss or theft of a personal device used to access University data.
- Circumventing or attempting to circumvent multi-factor authentication or conditional access controls.
- Using a jailbroken or rooted device to access University systems.
- Failure to securely delete University data from a personal device on departure from the University.
- Connecting a personal device to the corporate wired network without authorisation.

8.3 **Legal and regulatory obligations**
Breaches involving personal data, unauthorised access or other unlawful activity may be reported to external authorities where required, including law enforcement, the Information Commissioner's Office (ICO) and any organisation whose systems or data may have been affected.

9 Review

9.1 This policy will be reviewed annually by the Information Security Manager and approved by the IGSC. Reviews may be brought forward where there are significant changes to legislation, technology, the threat landscape or the University's operating environment.

Version control

Version	Date	Changes	Author
0.1	February 2026	Initial draft. Replaces SGUL BYOD policy. Aligned with AUP v0.1 and ISO 27001:2022.	[Author]

Normative references

- ISO/IEC 27001:2022 Annex A controls A.5.10, A.5.12, A.6.7, A.7.9, A.8.1, A.8.7, A.8.10, A.8.24
- NCSC guidance on securing personal devices and erasing devices
- Cyber Essentials technical requirements
- UK GDPR and Data Protection Act 2018
- JANET Acceptable Use Policy

This policy forms part of the University's ISMS suite governed by the Information Security Policy.

Policy information

Should you require further information regarding this policy or access to the policy in an alternative format, then please contact the Information Security Manager, cybersecurity@citystgeorges.ac.uk.

Policy Title:	Bring Your Own Device (BYOD) Policy
Policy Version:	1.0
Primary Author:	Information Security
Related Policies:	IT Acceptable Use Policy; Hardware Asset Management Policy; Data Protection Policy; Information Security Policy
Accountable Authority:	Chief Information Officer (CIO)
Approving Authority:	Information Governance & Security Committee (IGSC)
Date of Approval:	11th June 2026
Policy effective from:	11th June 2026
Date of Review:	8th June 2026

Appendix A – ISO 27001:2022 control mapping

Control	Title	How this policy addresses the control
A.5.10	Acceptable use of information	Sections 3.2, 3.4 – acceptable use of University data on personal devices and data classification restrictions.
A.5.12	Classification of information	Section 3.4 – data restrictions tied to information classification levels.
A.6.7	Remote working	Sections 3.5, 3.6 – controls for secure remote access from personal devices.
A.7.9	Security of assets off-premises	Sections 3.3, 3.5, 3.6 – device security, network restrictions and user responsibilities.
A.8.1	User endpoint devices	Sections 3.3, 3.9 – minimum security standards and MDM enrolment.
A.8.7	Protection against malware	Section 3.3 – anti-malware and firewall requirements.
A.8.10	Information deletion	Section 3.7 – secure deletion on departure or disposal.
A.8.24	Use of cryptography	Section 3.3 – full disk encryption required on laptops and desktops.