SOP Title Reference: **Bring Your Own Device (BYOD)**			
Author: **IT Services**		Approved by: **ISB**	

IT Services
IT Policies and Procedures

Bring Your Own Device (BYOD) Policy

IT Services, St George's, University of London, Jenner Wing, Cranmer Terrace, London SW17 0RE

Document History and Control

Version:	**V1 .2**
Policy Owner:	**IT Services**
Review cycle:	**Biennial**
Next Review Date:	**June 2025**
Responsible Committee:	**Information Systems Board**
Committee Approval Date:	

This document is subject to formal document version control and an entry should be made in the Document History table below defining changes.

Document History

Version	Date	Author	Rationale
1	**02.12.2019**	**IT Services**	**Last Revised**
1.1	**08.06.2023**	**IT Services**	**Updated version adopting version control. ISB (Information Systems Board) Jan 23.**
1.2	**08.06.2023**	**IT Services**	**Changes to reflect the implementation of MS Intune**

Contents

1. Introduction

This document is intended to address the use of un-managed devices in the workplace by SGUL members, e.g., smart phones, tablets, laptops and other such devices to connect to university resources, and to access and store University information, as well as their own. This practice is commonly known as ‘bring your own device’ or BYOD. The following terms and definitions will be used:

Term	Definition
Un-managed	A device that has not been configured by IT Services to access SGUL resources. This could be a personal device or SGUL device.
Personal Device	A device that is owned by the user
Corporate Device	A device that has been purchased and configured by IT Services.
SGUL Device	A device that has been purchased by SGUL but has not been configured for corporate access
Mobile device	Refers to any device that could be managed by the Mobile Device Management system, e.g., laptop, home PC, tablet, mobile phone etc

2. Purpose

As data controller SGUL must remain in control of the personal data for which it is responsible. SGUL members are required to keep secure University information and data they work with, and the use of non-university owned devices in this context creates issues that need to be addressed, particularly around data security.

It is also important for the University to safeguard the security, integrity and availability of its resources when being accessed by non-University devices.

The aim of this document is to

a) outline the circumstances under which it is acceptable to use BYOD to access University resources

b) define the categories of university information that can be stored and / or processed on non-University devices.

3. Scope

This policy applies to all SGUL members (staff, students, contractual third parties and any other authorised persons) who have access to SGUL information systems and other relevant IT-based resources.

BYOD shall be taken to mean any device used to access SGUL resources and information systems, that is either not owned by SGUL or is not managed centrally by the University, e.g., via the SGUL managed desktop.

4. Key Principles

Where BYOD's are used by SGUL members for work purposes this must be done in line with all other relevant University policies including, but not necessarily limited to, the Information Governance Framework, Information Management Policy, Information Security Policy, IT Conditions of Use and Data Protection Policy.

The contents of our systems and University data remain University property. All materials, data, communications and information, including but not limited to, e-mail (both outgoing and incoming), telephone conversations and voicemail recordings, instant messages and internet and social media postings and activities, created on, transmitted to, received or printed from, or stored or recorded on a device during the course of your work for the University or on its behalf is the property of the University, regardless of who owns the device.

University data held on personally owned devices is subject to the Freedom of Information Act and Subject Access rights under the Data Protection Act and must be provided to the Governance Manager or Data Protection Officer on request.

4.1 Device Security

SGUL employs a Mobile Device Management (MDM) platform to protect University infrastructure and data. All unmanaged devices that access company data must be enrolled in SGUL's MDM system. The MDM solution allows for centralised management and oversight, including the ability to remotely wipe devices in the event of loss or theft, enforce password policies, install necessary security apps, and monitor for unauthorised access.

To successfully enrol in the MDM a device must meet a minimum set of requirements. These requirements are set by SGUL.

You should not use devices owned by other people, or which are used by non-SGUL members, to connect to university resources.

Credentials required for logging onto university systems should not be stored on BYOD's except where the device is encrypted and configured to allow remote wiping, should it be lost or stolen. Where a device is not encrypted or set up for 'remote wipe' users must make sure they log out of university systems at the end of each session.

The University will not monitor the content of personal devices used to connect to its IT facilities or resources. However, SGUL reserves the right to

prevent access by any device that is considered a risk to its network or systems.

4.2 Data Security

Whilst personal devices may be used to access data, including work related emails, contained in university systems, there are restrictions on connectivity and what types of data can be physically stored on a personal device.

BYOD should never be plugged into the corporate network; Unmanaged devices on the corporate network pose a significant threat.

BYOD will not be allowed access to the corporate VPN; The VPN presents a device as if it exists on the corporate network and as such, an unmanaged device poses a serious threat.

Personal Identifiable Data should never be downloaded or stored onto a BYOD.

Other University information categorised as ‘Highly Confidential’ or ‘Restricted’ should never be downloaded or stored on BYODs.

If you are not sure of the categorisation of the data you are dealing with, please refer to the SGUL Data Classification Policy. This policy groups University data into 3 categories; Highly Confidential, Restricted and Public and provides detailed definitions of these categories.

There are no restrictions on the downloading and storing of university information categorised as ‘Public’ on personal devices.

5. Incident Management

It is the duty of all users to immediately report any actual or suspected breach in data security involving the use of the BYOD e.g., where the BYOD has been used to access University resources contrary to this policy and has subsequently been lost, stolen or otherwise ‘compromised,’ to the SGUL Data Protection Officer (DPO) either via:

- the data incident reporting form which can be found at https://www.sgul.ac.uk/about/our-professional-services/information-services/information-governance/data-protection :or
- emailing the DPO on dataprotection@sgul.ac.uk;

Staff members must also notify their line manager of the incident

You are required to co-operate with any investigation into a suspected breach, which may include providing us with access to the device.

6. Policy Compliance

If any user is found to have breached this policy, they may be subject to SGUL's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from IT Services.