London Business School

Acceptable Use Policy

Audience: This document is for anyone in the organisation, or who represents the organisation, who handles any type of data and uses any of the organisation's technology, business systems, or processes.

Document Owner: Information Security Manager

Release Date: v2.0; February 2024

Contents

1. Introduction

Information and Communications Technologies are essential to London Business School for its research, teaching, and administrative activities. These services are provided to authorised users on condition they are used for legitimate, authorised purposes, and in line with all applicable laws, regulations, and School policies.

The purpose of this policy is to define the acceptable use of London Business School's (the School's) IT Resources for legitimate purposes and to minimise the risk of their unauthorised access or misuse. 'IT Resources' includes but is not limited to School computer equipment, software, systems, networks, and information, as well as the systems, services and personal devices used to access School data.

2. Scope

This policy applies to all School information assets (documents, files, software, and hardware - digital or physical); to the systems or services used to access them (e.g., email or networks) and to all users of those School IT resources, including, but not limited to faculty, staff, participants, students, alumni, and third parties.

This policy relates to the use of IT devices, when connected to the School network (directly or indirectly), to all School owned information assets, including when stored on private systems, and to all information services provided to or by the School or an external agency.

This policy works in tandem with the acceptable use policy of our service provider, Jisc, which manages network connections between Universities and Colleges and the Internet. This includes any use of the Eduroam WiFi network, whether at the School or accessed elsewhere.

3. Terms of Use

3.1 IT Resources are provided for "Authorised use" (defined as use required to meet the purpose of an individual's registration, appointment, or employment with the School). Use of School IT Resources is conditional to compliance with applicable laws and School policies. Reasonable personal use of IT Resources is permitted where it complies with all aspects of this and all other School policies, and it does not disrupt or distract from the efficient conduct of School business.

3.2 IT Resources are provided at the risk of the user. London Business School provides no warranties or undertakings to the user, and accepts no liability for loss, damage or inconvenience arising directly or indirectly from the use of the resources, except where statutory health or safety matters are involved.

3.3 London Business School reserves the right to check for insecure and vulnerable systems and inspect, monitor, copy and/or remove user data or user access to investigate operational problems or for the detection and investigation of suspected misuse. This includes authorised interception and monitoring of communications as provided for by applicable law and in accordance with School policies, including the Monitoring Policy.

3.4 Any form of electronic communication may be construed in law as a publication. Users must be aware of the implications with respect to Intellectual Property Rights of publishing or using information in any electronic form.

4. Acceptable Use Policy

The following section outlines London Business School's policy on acceptable use of School IT Resources:

	You must	You MUST NOT
4.1 Physical Security of IT Resources You must take appropriate steps to protect all School devices, equipment, and hard copy materials from unauthorised access, misuse, or damage at all times.	• Store all devices, equipment, and hard copy materials securely when not in use. • Lock screens or log out of devices when not in use. • Ensure School information is only visible to authorised users. • Report a loss or theft of any LBS device, equipment, or hard copy materials immediately to databreach@london.edu.	• Leave devices, equipment, or hard copy data unattended in public places. • Carry out any activity that may damage or interfere with School devices or equipment.

4.2 Account Security

You may be issued with access to one or more IT accounts by LBS. You must ensure all accounts are kept secure and protected from misuse.

You must	You MUST NOT
• Use strong passwords (e.g., 'three random words'). • Where available, use multifactor authentication (MFA/2FA). • Use a secure method for storing passwords, such as a password manager. • Be vigilant when entering credentials. Check you are accessing legitimate sites and services. • Report compromise of your LBS credentials immediately to databreach@london.edu.	• Disclose or share access to IT accounts. • Use others' credentials or passwords or allow others to use yours. .

4.3 Use of LBS Devices, Systems & Networks

The School's devices, systems, and networks, including the Eduroam[1] and Janet[2] networks or other third-party service[3], must be used in compliance with this and all other LBS policies, regardless of how or where they are accessed from.

You must	You MUST NOT
• Only access IT Resources you are authorised to access, either School resources or external ones. • Maintain LBS devices as prompted, including timely reboots when prompted. • Only download or install LBS-provided or approved hardware or software to School devices, systems, or networks. • Use all materials and software in respect of any copyright or terms of use. • Report security incidents and data breaches immediately to databreach@london.edu. • Use Eduroam/Janet, either at your Home or visited organisation, in accordance with both Eduroam and the hosting institution's Conditions of Use.	• Undertake activities that attempt to gain unauthorised access to any IT system, disrupt IT services, introduce malicious software, or that may cause loss, damage, destruction, or a confidentiality breach of data. • Attempt to circumvent, alter, or remove any security settings, firewalls, software, or authentication processes, designed to protect School IT Resources. • Connect School devices to the internet using non-standard or insecure connections.

4.4 Use of Personal Devices to Access LBS Systems & Data

Where personal devices are used to access IT Resources and data, the School must be allowed to control the portion of the device that contains LBS data.

You must	You MUST NOT
• Ensure all devices used to access School IT Resources or data meet minimum security requirements, including use of a passcode / password, auto-device lock settings, etc. • All devices must be fully supported at both a hardware and operating system level by the manufacturer(s). • Immediately report the loss or theft of any non-LBS device that has a risk of School data being breached to databreach@london.edu.	• Store, maintain or backup School-owned information or data locally on non-LBS devices or removable media. Where required, users will have access to the LBS Office365 application suite where data should be stored.

4.5 Use of Email, Messaging & Collaboration Platforms

Use of School email, messaging, and collaboration platforms must be used in compliance with this and all other School policies, regardless of how or where they are accessed from.

You must	You MUST NOT
• Use School-provided or approved software and applications for LBS work and when sending or transmitting School information and data. • Only share information with individuals authorised to access it. • Be aware that information sent and received by or stored in School systems, including emails, are subject to freedom of information (FOI) requests and / or Data Subject Access Requests (DSARs). • Be vigilant to phishing emails or messages.	• Transmit any materials considered offensive, defamatory, libellous, harassing, threatening, or discriminatory. • Send or forward unsolicited emails, including junk emails and bulk email transmissions (spamming). • Send communications that attempt to impersonate or misrepresent another individual.

[1] https://community.jisc.ac.uk/library/janet-services-documentation/eduroamuk-policy
[2] https://community.jisc.ac.uk/library/acceptable-use-policy
[3] Use of third-party services is subject to the provider's terms of service. Information specific to the use of Library services can be found here - https://library.london.edu/important/terms

	You must	You MUST NOT
4.6 Use of the Internet & social media The internet and social media must be used in compliance with this and all other School policies and copyright laws.	• Respect the copyright of all materials used or referenced, including where the source of the material or data may be obscure such as the output of generative artificial intelligence.	• Use the internet or social media for the purposes of harassment or to make offensive, defamatory, libellous, harassing, threatening, or discriminatory remarks, or which otherwise might damage the School's reputation. • Access, publish, create, store, or transmit any material that is offensive, obscene, indecent, or unlawful, or which otherwise might damage the School's reputation. • Publish or post non-public LBS information or data on the internet or social media sites. • Register external domains without approval or associate LBS with any external facility that may damage the School's reputation.

	You must	You MUST NOT
4.7 Remote working When working at home or at any other non-School premises you must take appropriate steps to ensure School information is not compromised.	• Ensure any devices which store or have access to School data are locked before being left unattended.	• Discuss confidential matters in public or where others, including family or others living at the same location, can overhear them. • Allow anyone else to use a School-supplied device. • Allow unauthorised individuals, including family or others living at the same location, to access School information, devices, or systems.

5. Roles and Responsibilities

Chief Digital and Information Officer (CDIO)

- The CDIO is accountable for supporting the Acceptable Use Policy and ensuring compliance is met throughout the organisation.

Information Security Manager

- The Information Security Manager owns the policy and is responsible for ensuring that appropriate controls are defined and implemented throughout the organisation and any exceptions and risks are managed.

Senior Data Privacy Manager

- The Senior Data Privacy Manager is responsible for ensuring that this policy services the needs of protecting data in relation to privacy and the rights of Faculty, Staff, and students.

Data Privacy & Security Committee

- Led by the CDIO this is a multidisciplinary group that reviews, endorses, and supports the implementation of changes to the Acceptable Use Policy and related standards and processes.

All School Employee, Faculty, Contractors, Students, Participants and Alumni

- All School Employees, Faculty, Contractors, Students, Participants and Alumni are responsible for complying with this policy.
- They are required to complete any training related to the subjects covered in this policy and are responsible for making informed decisions in relation to the acceptable use of the School's information and data assets.

6. Compliance and Exemptions

London Business School will conduct periodic monitoring of compliance against the organisation's information security policies, standards, procedures, and controls to ensure they are adequate, effective and being adhered to.

Where controls are not met this will be documented and assessed in line with the School's appetite for risk. Where risks exist, this will be managed in line with LBS's Risk Management processes where escalation, treatment and further controls will be determined.

Purposeful violation of this policy may be subject to disciplinary action, up to and including termination of employment or removal from courses. Serious breaches may lead to criminal or civil proceedings.

Exemptions to this policy may be granted subject to the approval of the CDIO. All exemption requests shall be recorded along with their outcome.

7. Review and Continual Improvement

This policy will be reviewed periodically and after significant organisational and business system change. It will be reviewed considering the latest changes to regulation, legislation and industry best practise and promotes the need for continual improvement. The review will consider that this policy:

- Remains operationally fit for purpose.
- Reflect changes in technologies or business processes.
- Are aligned to industry good practice; and
- Support continued regulatory, contractual, and legal compliance.

8. Document Control

Document Information

Title	LBS Acceptable Use Policy
Author	Information Security Working Group
Approver	Chief Digital & Information Officer; Data Privacy & Security Committee
Owner	Information Security Manager

Version History

Version	Date	Summary of Changes
Published	September 2021	Approved and published policy
v2.0	February 2024	Full policy refresh.