Global Banking School
+44 (0) 207 539 3548

info@globalbanking.ac.uk

www.globalbanking.ac.uk

891 Greenford Road, London

UB6 0HE

GBS IT Acceptable Usage Policy

Document title	GBS IT Acceptable Usage Policy
Version	V1.0
Approved by (Oversight Committee)	Information Management Group (IMG)
Policy lead (Staff member accountable)	Managing Director
Date of original approval	January 2025
Date of last review	NA
Changes made at the last review:	NA
Date effective from	January 2025
Date of next review	January 2028

Related policies

- GBS Password Policy
- GBS ICT Policy
- GBS Equality and Diversity Policy
- GBS Freedom of Speech Code of Practice
- GBS Anti-Harassment and Anti-Bullying Policy – Staff, Students
- GBS Student Charter
- GBS Student Disciplinary Policy and Procedure
- GBS Staff Disciplinary Policy
- GBS Email Usage Policy
- GBS Data Protection Policy

External Reference

1. Device Security Guidance, accessed online at: https://www.ncsc.gov.uk/collection/device-security-guidance/policies-and-settings/antivirus-and-other-security-software

2. Small Business Guide: Cyber Security , accessed online at : https://www.ncsc.gov.uk/collection/small-business-guide/protecting-your-organisation-malware

Contents

Global Banking School IT Acceptable Usage Policy

1. Introduction/Policy Statement

1.1. This document outlines the IT Acceptable Usage Policy and guidance.

2. Purpose

2.1. The purpose of this policy to communicate to all users what is acceptable and unacceptable behaviour when using Global Banking School IT Systems, networks, and equipment. IT Acceptable Usage Policy protects confidentiality, integrity, and availability of GBS IT resources.

2.2. A detailed policy on usage of Personal devices by Staff and Students is available as GBS Bring Your Own Device (BYOD) Staff Policy and GBS Bring Your Own Device (BYOD) Student Policy

3. Scope

3.1. This policy is applied to all GBS users (staff / students), managed services and third party who uses GBS IT Resources.

3.2. The term GBS User mentioned in this policy refers to staff, students, research assistants, visitors/anyone using GBS IT resources. The term institution refers to Global Banking School Limited. The term GBS IT Device refers to any IT device or system owned by GBS including but not limited to laptops, desktops, mac books, mobile phones, tablets, projectors etc.

4. Terminology

4.1. Shall or Must – This term is used to state **a mandatory** requirement of this policy.

4.2. Should – This Term is used to state a **recommended** requirement of this policy.

4.3. May – This term is used to state an **optional** requirement of this policy.

4.4. Shall not or must not- This term is used to state an **absolute prohibition** requirement of this policy.

4.5. Should not – This term is used to state a **not recommended** requirement of this policy.

5. Policy

5.1. The GBS IT Acceptable Usage Policy applies to:

- **GBS Staff** using **GBS IT devices** to login GBS applications/network.
- **GBS Staff** using **Personal device** to login GBS applications/network
- **GBS Student** using **GBS Lab or Classroom IT devices** to login GBS applications /network.
- **GBS Student** using **Personal device** to login GBS applications/network
- **Anyone** not mentioned above and is using **GBS IT Resources.**

5.2. All GBS users (staff/research assistants/students/visitors/anyone using GBS IT resources) must follow and adhere to the following policy statements to access GBS IT Resources:

Acceptable Use:

GBS User must	**adhere to all company policies**
GBS User must	**use credentials like password to login to GBS IT devices or systems along with Multi Factor Authentication wherever applicable**
GBS User must	**safeguard IT Credentials (Password/MFA Code/Login token)**
GBS User must	**use own username and password.**
GBS User must	**check and update GBS IT Devices (Laptop/Desktop) Software not exceeding 14 days. Restart device on getting alert for updates pushed out by IT Team.**
GBS User must	**keep security software on GBS IT devices (like WatchGuard EPDR) preinstalled by IT team running in background and updated.**
GBS User must	**lock their GBS IT Devices’ (laptop/desktop) screen while moving away from desk.**
GBS User must	**scan removable Media (like USB Stick) by Anti-Virus/Anti Malware before use.**
GBS User must	**remove or uninstall applications no longer needed from GBS IT Devices with support of GBS IT Team.**
GBS User must	**remove or uninstall End of Life applications from GBS IT Devices with support of GBS IT Team.**
GBS User must	**take support from GBS IT Support for installation of any additional application on GBS IT Device.**

GBS User must	contact IT Support before download of blocked mails marked with high severity.
GBS User must	adhere to GBS Bring Your Own Device (BYOD) Staff Policy and GBS Bring Your Own Device (BYOD) Student Policy if personal devices are used to access GBS resources.
GBS user must	be diligent and careful on what he or she post on social media.
GBS User must	return all GBS IT Assets and devices upon End of Employment.

Unacceptable Use:

GBS User must not	reveal his or her password to others.
GBS User must not	use someone else's username/password.
GBS User must not	access unauthorised data.
GBS User must not	leave password exposed.
GBS User must not	store institution data on unauthorised devices and personal cloud space.
GBS User should not	connect GBS IT devices to network which are not approved or authorised by GBS IT Team.
GBS User must not	install software on their own on GBS IT devices or systems.
GBS User must not	send unsolicited bulk mails.
GBS User must not	use GBS email id on sites not relevant to work.
GBS User must not	change settings on any software installed on GBS IT devices by GBS IT Team.
GBS User must not	store organization information on removable media without authorisation and encryption.
GBS User must not	use GBS email or GBS internet or GBS IT devices for the purpose of harassment or abuse.
GBS User must not	use GBS email or GBS internet or GBS IT devices to gamble or for gaming.
GBS User must not	use GBS email or GBS internet or GBS IT devices to access, download, send or receive any data considered as sexually explicit, obscene, pornographic, discriminatory, racist, defamatory, seditious, homophobic, blasphemous, abusive, or illegal.

GBS User must not	**use GBS email or GBS internet or GBS IT devices to advocate or promote any unlawful act.**
GBS User must not	**post messages or material on social media that could damage institution's reputation.**
GBS User must not	**attempt to monitor the use of GBS IT devices, systems, or IT Infrastructure without explicit authority.**

5.3. This policy should be read in conjunction with the accompanying **IT Acceptable Use Policy (Guidance).**

6. Monitoring

6.1. GBS monitors and records the use of IT systems.

6.2. Under the Telecommunications (Lawful Business Practice [LBP]) (Interception of Communications) Regulations 2000 (Statutory Instrument 2000 No.2699) GBS reserves the rights to monitor users' activities to:

- Record evidence of official transactions
- Ensure compliance with regulatory or self-regulatory guidelines (including this Policy)
- Maintain effective operations of systems (for example, preventing viruses)
- Prevent or detecting criminal activity
- Prevent the unauthorised use of computer and telephone systems to ensure that the users do not breach GBS policies.

6.3. Under this regulation there is a requirement for employers to inform staff and users about such monitoring. The publishing of this Policy is one means of fulfilling that obligation

7. Non-Compliance

7.1. GBS User who violate this policy may face disciplinary consequences in proportion to their violation. Management will decide how severe offense is and take the appropriate action.

8. Data Protection and Confidentiality

8.1. GBS is registered with the Information Commissioner's Office as a Data Controller. Details of GBS's registration is published on the Information Commissioners website. GBS as a Data Controller shall implement appropriate technical and organisational measures to ensure that processing of personal information is performed in accordance with the UK General Data Protection Regulations (UK GDPR) and under the Data Protection Act 2018 (DPA)

8.2. The UK GDPR and DPA regulates the use and storage of personal information (i.e., any information which identifies a living individual) on computing systems. It is the user's responsibility to ensure that their information and computer usage complies with this law. Failure to do so could result in criminal charges being brought against both user and GBS.

9. Policy Review

9.1. This policy may be amended by GBS at any time and will be reviewed annually to ensure it is fit for purpose. Any issues related to the monitoring and review of this policy, please contact asqo@globalbanking.ac.uk.

10. Alternative Format

10.1. This policy can be provided in alternative formats (including large print, audio and electronic) upon request. For further information, or to make a request, please contact the Academic Standards and Quality Office at asqo@globalbanking.ac.uk.

Appendix 1: Glossary

GBS: Global Banking School

IT: Information Technology

BYOD: Bring Your Own Device

ICT: Information and Communications Technology

MFA: Multifactor Authentication

PIN: Personal Identification Number

GDPR: General Data Protection Regulation

DPA: Data Protection Act

NCSC: National Cyber Security Centre