GBS IT Acceptable Usage Guidance

This article is an added guidance on GBS IT Acceptable Usage Policy. The GBS IT Acceptable Usage Policy applies to all users and the term GBS User mentioned in this document refers to staff, students, research assistants, visitors/anyone using GBS IT resources. Term GBS IT Device refers to any device or system owned by GBS including but not limited to laptops, desktops, mac books, mobile phones, tablets, projectors etc

Acceptable Use

GBS
GLOBAL BANKING SCHOOL

IT ACCEPTABLE USAGE GUIDANCE
DO'S

Adhere to all company policies

Use Credentials to login- Password and MFA

Safeguard Credentials

Use own username and password

Verify and update laptop software within a 14-day timeframe.

Scan removable media by Anti-Virus Software before use

Ensure anti-virus software (like Watchguard EDPR) is running on your GBS Devices

be deligent and careful on social media posts

For GBS Devices, take support of IT services and

do remove unsupported apps

do remove apps no longer needed

install additional apps

BYOD

Personal Devices

adhere to
GBS Bring Your Own Device Staff Policy &
GBS Bring Your Own Device Student Policy
to access GBS resources using personal devices

Return IT assets upon end of employment

Unacceptable Use

- All GBS Users are also bound by GBS's IT policies, when using GBS IT services systems, available at https://www.globalbanking.ac.uk/about-us/our-policies

- Personal data if any may be wiped off when device is reported as compromised or lost as well as during surrender of GBS IT devices during change of device or return upon end of employment.

- Do not use and upload GBS Institution data on third party applications and web services without approval from IT Systems Team as well as Information Security Team.

- GBS User must not send or post messages or material on social media that could damage institution's image or reputation – this extends to commenting on or reposting of others content. Only staff who have been authorised to use the company's social networking accounts may do so. Allowing only designated people to use these accounts ensures the company's social media presence is consistent and cohesive.

- GBS User must not attempt or try to check the use of GBS IT devices, systems or IT infrastructure without explicit approval from Head of Information Technology and Services. This includes but not limited to:
    - Network/device discoveries or scanning.
    - Wireless traffic capture.
    - Network Traffic Monitoring.
    - Use of key logging software.
    - Penetration testing.
    - Attempt to access server or system logs.