Document title	GBS ICT Policy
Oversight Committee	Executive Board
Policy lead (Staff member accountable)	Managing Director
Approved by	Executive Board
Approval date	March 2019
Date effective from	March 2019
Date of next review	March 2025
Version	2.0

Related GBS policies
GBS Data Protection Policy
GBS Safeguarding and Prevent Policy
GBS Equality and Diversity Policy
GBS Freedom of Speech Policy
GBS Anti-Harassment and Anti-Bullying Policy
GBS Student Charter

5. UK Public General Acts, *Counter-Terrorism and Security Act 2015*, Accessed online at: https://www.legislation.gov.uk/ukpga/2015/6/section/26

6. GOV.UK Statutory Guidance, *Prevent duty guidance*, Accessed online at: https://www.gov.uk/government/publications/prevent-duty-guidance

7. UK Public General Acts, *The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000*, Accessed online at: https://www.legislation.gov.uk/uksi/2000/2699/contents/made

Contents

Global Banking School ICT Policy

1. **Policy Statement**

    1.1. Global Banking School (GBS) recognises the vital role information technology plays in GBS missions and related administrative activities as well as the importance in an academic environment of protecting information in all forms. As more information is used and shared in a digital format by students and staff, both within and outside GBS, an increased effort must be made to protect the information and the technology resources that support it. Increased protection of our information and Information Technology Resources to assure the usability and availability of those resources is the primary purpose of this Policy. The Policy also addresses code of practice for the use of IT facilities at GBS.

2. **Purpose**

    2.1 The purpose of this policy is to inform GBS staff, students, visitors, and other stakeholders the use of information computing technology facilities owned and provided by GBS.

    2.2 This policy concerns all computer systems, networks and Wi-Fi facilities operated by GBS at all its campuses and regardless of location, where responsibility for user management and control resides with members of staff of GBS, or where it may be outsourced to third parties. This policy has been developed to help ensure that GBS information computing technology, in its widest sense, is protected against unauthorised use and unauthorised access. In particular, the policy has been developed to help ensure protection against una
    systems.

3. **Scope**

    3.1 This policy applies to:

    All full-time, part-time, and temporary staff employed by, or working for or on behalf of GBS

    All students studying at GBS

    Contractors and consultants working for GBS

    All other individuals or groups, including visitors, who have been granted access to

e

6. Computer Crime and Misuse

6.1 GBS expects users to use ICT facilities, and in particular email and the Internet, responsibly at all times. Suspected computer crime and misuse of GBS ICT facilities, including excessive personal use by staff, will be investigated by the Managing Director and action taken accordingly.

7. Monitoring use of GBS ICT Facilities

7.1 Under the Telecommunications (Lawful Business Practice [LBP]) (Interception of Communications) Regulations 2000 (Statutory Instrument 2000 No.2699) GBS reserves

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.

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

8. Policy Review

8.1 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.

9. Data Protection and Confidentiality

9.1 GBS

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).

9.2 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 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 you and GBS.

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: