+ 44 (0) 207 539 3548
info@globalbanking.ac.ulk
www.globalbanking.ac.uk
153-159 Bow Road, London, E3 2SE

GBS Code of Practice for the use of Information Computing Technology Facilities (ICT)

GBS

Code of Practice for the use of Information Computing Technology Facilities (ICT)

Contents

1. Purpose

1.1 To provide a policy for the use of information computing technology facilities owned and provided by GBS for staff, students and other stakeholders.

2. Scope, background and applicability

2.1 Scope

This ICT Policy concerns all computer systems, network and wifi 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.

2.2 Background

This policy document has been developed to help ensure that GBS's 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 unauthorised access and modification to GBS' various data systems and other ICT systems.

2.3 Applicability

This policy concerns:

- The use of GBS owned ICT facilities, including information systems
- GBS network facilities (wired and wireless) regardless of whether these are used through the connection of GBS owned equipment or through the connection of private equipment to GBS owned equipment.

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 the GBS

- Contractors and consultants working for GBS
- All other individuals or groups, including visitors, who have been granted access to GBS's ICT facilities.

It is the responsibility of each person to whom this policy applies to fully adhere to its requirements.

3. Code of practice for the use of ICT facilities at GBS

3.1 Conditions of use of GBS' computer systems

You may use GBS's ICT and wifi facilities if you have been authorised and are:

- An employee of GBS
- A student registered for a programme of study at GBS
- A former member of staff
- An individual or a member of a group who has been permitted to use the GBS' ICT
- A visitor to GBS.

Only the Chief Executive Officer or Managing Director may authorise individuals or groups to use and access GBS's facilities.

3.2 Use of private equipment

Privately owned equipment of staff, students and other individuals or groups may only be connected to GBS' wifi upon agreement of either the Chief Executive Officer or Managing Director of GBS. GBS accepts no responsibility for the effects that any such connection may have on the operability of privately owned electronic or other devices, consequently all risks, however small, reside with the owner.

3.3 Laws and regulations

All use of GBS's ICT facilities must be in full compliance with English law, and where appropriate, all other regulations which are applicable. You must not try to gain unauthorised access to any computer system anywhere at GBS. This is commonly known as hacking and constitutes a criminal offence under The Computer Misuse Act 1990. In certain cases, such activities can also be contrary to other legislation, for example, The Terrorism Act 2000.

You must not do anything maliciously, negligently or recklessly which might cause any sort of harm or disruption to any computer system anywhere (worldwide), or to any of the programs or data on any system. In this context the word harm is taken to mean any kind of damage, and any kind of unauthorised access, denial of resources or any data alteration.

If you are reasonably requested to do so, you must justify your use of GBS' ICT facilities and/or wifi facilities. You must explain (in confidence, if necessary) what you are doing, and how and why you are doing it. You must make any reasonable changes requested by senor staff and comply with any reasonable restrictions placed upon you.

You must comply with valid regulations covering the use of software and datasets,

whether those regulations are made by law, by the producer or supplier of the software or datasets, by GBS, or by any other legitimate authority. Where you have any doubts you must contact the Chief Executive Officer or Managing Director before using GBS' ICT facilities.

The Data Protection Act 1998 regulates the use and storage of personal information (i.e. any information which identifies a living individual) on computing systems. It is your responsibility to ensure that your information and computer usage complies with this law. Failure to do so could result in criminal charges being brought against both you and GBS.

Whilst every reasonable endeavour is made to ensure that the ICT facilities and wifi facilities are available as publicised and scheduled and function correctly, no liability whatsoever can be accepted by GBS for any direct or consequential losses or delays as a result of any system malfunction.

3.4 Conditions applicable to all GBS ICT users

GBS' ICT facilities must not generally be used for, or in connection with, the activities identified below, some of which could result in legal action or civil proceedings being mounted against either an individual, GBS, or both.

(a) Deliberately accessing, creating or transmitting any obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material, with the exception of data which is connected with GBS work or official research or other professional activity, where the sender/recipient would expect to exchange such material with other users in a professional capacity;

(b) Creating, transmitting or accessing material which is designed or likely to cause offence, annoyance, inconvenience or needless anxiety to another

(c) Creating, transmitting or accessing material which runs the risk of drawing people in to, or towards, terrorism and/or extremism, except where it can be demonstrated that there is a legitimate academic interest

(d) Deliberately contributing to News Groups or web sites that advocate illegal activity

(e) Creating or transmitting defamatory material or material that is libelous of any other person's or company's reputation, products or services;

(f) Viewing, transmitting, copying, downloading or producing material, including (but not exhaustively) software, films, television programmes, music, electronic documents and books which infringes the copyright of another person, or organization

(g) Making offensive or derogatory remarks about staff, students or GBS on interactive social and life-style websites such as Facebook and Twitter.

(h) Posting offensive, obscene or derogatory photographs, images, commentary or soundtracks on interactive social and life-style websites such as Facebook, Twitter and YouTube

(i) Transmitting or producing material which breaches confidentiality undertakings

(j) Attempting to gain deliberate access to facilities or services which you are unauthorised to access

(k) Deliberately undertaking activities that corrupt or destroy other users' data; disrupt the work of other users, or deny network resources to them; violate the privacy of other users; waste staff effort or networked resources

(l) Creating or transmitting unsolicited commercial or advertising material unless that material is part of a service to which recipients have chosen to subscribe

(m) Making commitments via email or the Internet on behalf of GBS without full authority

(n) Undertaking any activities detrimental to the reputation or business interests of GBS

(o) Initiating or participating in the sending of chain letters, 'junk mail', 'spamming' or other similar mailings.

Any user who inadvertently accesses an inappropriate Internet site must immediately close the session or return to the previous page.

Any member of staff who receives an inappropriate email message or e-mail content that appears to have been sent by a member of staff or student may wish to report the matter to the Chief Executive Officer or Managing Director.

3.5 Computer crime and misuse

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's ICT facilities, including excessive personal use by staff, will be investigated by the Managing Director and action taken accordingly.

4. Monitoring use of GBS' ICT facilities

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.

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.

5. Related GBS Policies

The following policies should be noted and read in conjunction with this GBS ICT Policy:

- GBS Safeguarding and Prevent Policy
- GBS Equality and Diversity Policy
- GBS Freedom of Speech Policy
- GBS Anti-Harassment and Anti-Bullying Code of Practice
- GBS Student Charter
- GBS Student Disciplinary Policy and Procedure
- GBS Student Handbook
- GBS Staff Handbook

A&QD 30 November 2019
Version 1.1