Global Banking School
+44 (0) 207 539 3548
info@globalbanking.ac.uk
www.globalbanking.ac.uk
891 Greenford Road, London
UB6 0HE

GBS Anti-Spam and Anti-Virus Policy

Document title	GBS Anti-Spam and Anti-Virus Policy
Version	V2.1
Approved by (Oversight Committee)	Board of Directors
Policy lead (Staff member accountable)	Managing Director
Date of original approval	March 2019
Date of last review	December 2024
Changes made at the last review:	Minor editorial changes (December 2024)
Date effective from	December 2024
Date of next review	December 2026

Related GBS policies

- GBS Data Protection Policy
- GBS Equality and Diversity Policy
- GBS Freedom of Speech Policy
- GBS Anti-Harassment and Anti-Bullying Policy
- GBS Student Disciplinary Policy and Procedure
- GBS Staff Disciplinary Policy
- GBS Email Usage Policy
- GBS CCTV Policy and Procedure
- GBS Social Media Policy
- GBS Whistleblowing Policy

External Reference Points

1. Information Commissioner's Office, Accessed online at: https://ico.org.uk/
2. UK Public General Acts, *Data Protection Act 2018*, Accessed online at: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
3. UK Public General Acts, *Computer Misuse Act 1990*, Accessed online at: https://www.legislation.gov.uk/ukpga/1990/18/contents
4. UK Public General Acts, *Terrorism Act 2000*, Accessed online at: https://www.legislation.gov.uk/ukpga/2000/11/contents
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 Anti-Spam and Anti-Virus Policy

1. Policy Statement

1.1. Global Banking School (GBS) recognises the vital role information technology plays in GBS missions as well as the importance in an academic environment of protecting information in all forms. ICT facilities are primarily provided to enable students and staff to perform their duties and to better conduct the business of GBS.

2. Purpose

2.1 The purpose of this policy is to ensure that all staff, students, visitors, or any individual using GBS systems are aware of their responsibilities in relation to safeguarding the confidentiality, integrity, and availability of data and software within GBS.

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 GBS ICT facilities.

3.2 Every individual defined within the scope of this document is responsible for the implementation of this policy whilst operating any IT equipment to access any of GBS systems.

4. Anti-Spam and Anti-Virus Checks

4.1 GBS will apply many anti-spam and anti-virus checks to incoming email. These checks are applied at the GBS mail relays, through which most of our incoming mail passes.

4.2 **Local Blacklists**

4.2.1 The address and name of the sending system is looked up in a local blacklist and the message is rejected if there is a match.

4.3 **Public Blacklists**

4.3.1 The address of the sending system is tested against various public blacklists. These blacklists have been chosen because they are known to be effective, have a reputation for few false positives (that is mistaken listings), have suitable listing methodologies, and provide good information on why particular addresses have been blacklisted. We use three public blacklists.

4.4 **Whitelisting**

4.4.1 If a blacklisted site needs to get mail through to us, we will generally expect them to fix the problem that lead to their being listed and delist themselves.

5. Intrusion Detection Architecture

5.1 **Stage 1 Anti-virus checking**

5.1.1 All messages are scanned for viruses, worms, etc., using our chosen Tier 1 Anti-virus software. If a virus is detected which appears on a list of those known to forge sender addresses, the message is simply discarded, as rejecting it would cause an error message to be sent to an innocent third party. Otherwise, the message is rejected.

5.2 **Stage 2 AV checking: Second tier AV**

5.2.1 Messages that make it past Tier 1 AV are then scanned using an open-source Tier 2 anti-virus scanner, which can pick up some malware that Tier 1 provider does not (and vice versa). It also can detect some classes of "phishing" messages (malicious messages attempting to fool victims into entering their financial details into bogus websites).

5.3 **Tier 2 AV scanner website**

5.3.1 The use of two virus scanners makes the service more robust. One or the other can go down, and messages can still be allowed through with confidence. Since they will update their signature databases with different frequencies and timeliness, this will also tend to narrow the window of vulnerability where a new virus can sneak in before signatures for it are available.

5.4 **Spam filtering with SpamAssassin**

5.4.1 SpamAssassin is a popular open-source software package which applies a variety of textual and other tests to messages in order to estimate the likelihood that they are spam. This likelihood is represented as a number, the spam score. SpamAssassin

assigns a score to each message it sees, which can subsequently be used to determine the message's disposition.

5.4.2 SpamAssassin is run on the main GBS mail relays. It scans all messages coming into the mail relays from networks outside of GBS. It adds headers to a scanned message containing indications of the spam score assigned to it, and the mail system then continues processing the message as normal.

5.5 **Thresholds**

5.5.1 The main control over the spam filtering is a number called the threshold. Messages rated with a score equal to or greater than the threshold are filed in the likely spam folder; messages rated less than the threshold are not affected and will be delivered to your inbox (unless there are subsequent filtering rules in place which might affect it).

5.5.2 At any given threshold there is always a chance that a spam message is filed in your inbox (a false negative) and a chance that a non-spam is filed in the likely spam folder (a false positive). If you increase the filtering threshold, the chance of false negatives increases, so more spam gets through to your inbox. At the same time, the chance of false positives decreases, so less non-spam mail is filed along with the spam.

5.5.3 Where the threshold should be set depends on the sort of email that each user receives. If you receive mail that tends to score highly, such as HTML-formatted newsletters, commercial announcements, and so on, you may prefer a higher threshold to allow this mail through to your inbox while accepting that a higher amount of spam will get through with it. If you receive only relatively "clean" mail, you may prefer a lower threshold. You may also prefer a lower threshold if you are prepared to check your likely spam folder often, while a higher threshold would allow you to check it less often.

6. Monitoring and Review

6.1 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.

7. Data Protection and Confidentiality

7.1 GBS is registered with the Information Commissioner's Office as a Data Controller. Details of the School's registration are 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).

7.2 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 you and GBS.

8. Alternative Format

8.1 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.