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

GBS Data Breach Policy

Document title	GBS Data Breach Policy
Version	V1.1
Approved by (Oversight Committee)	Board of Directors
Policy lead (Staff member accountable)	Data Protection Officer
Date of original approval	February 2022
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	November 2026

Related GBS policies
GBS Data Protection Policy GBS Equality and Diversity Policy GBS Freedom of Speech Code of Practice GBS Anti-Harassment and Anti-Bullying Policy GBS Student Disciplinary Policy and Procedure GBS Staff Disciplinary Policy GBS Support to Study Policy GBS Student Charter GBS Privacy Policy GBS Email Usage Policy
External Reference Points
1. 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, *Equality Act 2010*, Accessed online at: https://www.legislation.gov.uk/ukpga/2010/15/contents

Contents

Global Banking School Data Breach Policy

1. Introduction and Scope

1.1 Global Banking School (GBS) collects, holds, processes, and shares personal data. GBS attaches great importance to the secure management of the data it holds and generates. GBS could potentially hold staff accountable for any inappropriate mismanagement or loss of it. Every care is taken to protect personal data from incidents (either accidentally or deliberately) to avoid a data protection breach that could compromise security. GBS holds a variety of sensitive data including personal information about students and staff. If you have been given access to this information, you are reminded of your responsibilities under the GBS Data Protection Policy.

1.2 Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative non-compliance, and/or financial costs. To reiterate the importance of this policy, GBS i278(for 1d0.pio)-1 0 0 1 259.3eh2 you and/or financial costs.

2.2 To adhere to the UK GDPR and UK Data Protection laws and to have robust and adequate procedures and controls in place for identifying, investigating, reporting, and recording any data breaches.

2.3 To develop and implement adequate, effective, and appropriate technical and organisational measures to ensure a high level of security with regards to personal information.

3. Types of Breach

3.1 For the purpose of this Data Breach policy, data security breaches include both confirmed and suspected incidents. An incident in the context of this policy is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to GBS information assets and / or reputation.

3.2 Any copying or original creation of sensitive data and information onto any form of portable media transport device or mechanism (Memory Stick, CD, DVD, External Hard Drive, PDA, portable music player, Laptop, etc.) or its transportation beyond the secure environment it was intended to be used within (systems environment, PC environment, campus, office etc) carries additional responsibilities for the individual undertaking such activity. The removal of personal data, as identified by UK GDPR or the UK Data Protection Act 2018, by staff, contractors, and learners, shall not occur unless prior approval has been granted by the GBS Senior Management Team or the Data Protection Officer.

3.3 The following is a list of examples of breaches of security and breaches of confidentiality. It is neither exclusive or exhaustive and should be used as a guide only. If there is any doubt as to what constitutes an incident, it is better to inform your line manager who will then decide whether a report should be made. An incident includes but is not restricted to, the following:

loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g., loss of laptop, USB stick, iPad / tablet device, or paper record).

Loss of computer equipment due to crime of carelessness.

equipment theft or failure.

system failure.

unauthorised use of access to or modification of data or information systems.

attempts (failed or successful) to gain unauthorised access to information or IT system(s).

Finding doors and/or windows broken and/or forced entry gained to a secure room/building in which computer equipment exists.

unauthorised disclosure of sensitive / confidential data.

website defacement.
hacking attack.
unforeseen circumstances such as a fire or flood.
human error.

organisation who holds it.

3.4 A breach of confidentiality may include:

Finding confidential/personal information either in hard copy or on a portable media device outside GBS premises or common areas.
Finding any records about a staff member, student, or applicant in any location outside the GBS premises.
Passing information to unauthorised people either verbally, written or electronically.

3.5 A security incident is any event that has resulted or could result in:

The disclosure of confidential information to any unauthorised person.
The integrity of the system or data being put at risk.
The availability of the system or information being put at risk.

3.6 These responsibilities should be clarified by performing a risk analysis, which considers the following rules/principles:

3.7 Employee/Student (personal) data should never leave the campus. In this

location. Remote access to such data through an individual approved access levels and permissions is distinct and not intended to be included in the term

3.8 If it is a unique or master version of data/information that has not been safely copied to a secure electronic or physical location or environment within IT Security environment (implying that its subsequent loss is irrecoverable) then a copy should be made and stored securely prior to its off-site transportation for use.

3.9 Personal data (including about applicants, learners, and employees) shall not be emailed in raw data format either internally or externally to and from GBS. Personal data should be shared via password protected cloud-based files and locked down within servers, intranet, and cloud services with password protections as a minimum layer of security.

3.10 Personal data shall not be printed into hard copy and be left visible other than

hard copy documents containing personal data must be destroyed by shredding.

4. Reporting an Incident

4.1 Any individual who accesses, uses, or manages GBS information is responsible for reporting data breaches and information security incidents immediately to the Data Protection Officer at dpa@globalbanking.ac.uk or alternatively their GDPR representative for each department which is your line manager or Head of department.

4.2 All incidences of loss or theft of confidential information should be reported so that they may be investigated. A data or IT security incident relating to breaches of security and/or confidentiality could range from computer users sharing passwords to the loss or theft of confidential information either inside or outside GBS. If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable.

4.3 The report must include full and accurate details of the incident, when the breach occurred (dates and times), place of the incident, who discovered the incident, category/classification of the incident, action already taken if risk to GBS. Any action taken by the person discovering the incident at the time of discovery, e.g., report to police, details of who is reporting it, if the data relates to people, the nature of the information, and how many individuals are involved. The GBS Data Breach Incident Report Form should be completed as part of the reporting process *(refer to Annex 2).* Also please refer to the GBS Data Breach Incident Report Flowchart *(Annex 3).*

4.4 All staff should be aware that any breach of Data Protection legislation may result in the GBS Disciplinary Procedures being instigated.

5. Containment and Recovery

5.1 The Data Protection Officer (DPO) will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.

5.2 An initial assessment will be made by the DPO in liaison with relevant manager(s) to establish the severity of the breach and who will take the lead investigating the breach, (this will depend on the nature of the breach; in some the DPO in

6.3 An investigation will be undertaken by the DPO immediately and wherever possible, within 24 hours of the breach being discovered / reported.

6.4 The DPO will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

6.5 The investigation will need to consider the following:

the type of data involved.
its sensitivity.
the protections are in place (e.g., encryptions).
what has happened to the data (e.g., has it been lost or stolen.
whether the data could be put to any illegal or inappropriate use.
data subject(s) affected by the breach, number of individuals involved and the potential
effects on those data subject(s).
whether there are wider consequences to the breach.

7. Breach Notifications

7.1 GBS recognises our obligation and duty to report to the Information any data breaches in certain W*n1.92 re 0 0 1 180.02 464.8 Tm0 g0

10. Record Keeping

10.1 All records and notes taking during the identification, assessment and investigation of the data breach are recorded and authorised by the Data Protection Officer and are retained for a period of 6 years from the date of the incident. Incident forms are to be reviewed annually to assess for patterns or breach reoccurrences and actions taken to prevent further incidents from occurring.

11. Policy Review

11.1 This policy will be updated as necessary to reflect best practice and to ensure compliance with any changes or amendments to relevant legislation.

12. Data Protection Policy Breach

12.1 GBS takes compliance with the Data Protection policy very seriously, therefore a breach of this policy could potentially be treated as misconduct and could result in disciplinary action including in serious cases, dismissal. If staff or students are found to be in breach of this policy, GBS has the authority to revoke your access to our systems, whether through a device or otherwise. Failure to comply with the policy can lead to:

Damage and distress being caused to those who entrust us to look after their personal data, risk of fraud or misuse of compromised personal data, a loss of trust and a breakdown in relationships with GBS.

Damage to GBS reputation and its relationship with its stakeholders (including research funders and prospective students and collaborators).

13. Criminal Offence

13.1 A member of staff or student who deliberately or recklessly misuses or discloses personal data held by GBS without proper authority could lead to a criminal offence. Failure to comply with the policy carries the risk of significant civil and criminal sanctions.

14.2 The Data Protection Officer is responsible for regular compliance audits and gap analysis monitoring and the subsequent reviews and action follow ups. There is a continuous audit trail of all compliance reviews and procedural amendments and feedback to ensure continuity through each process and task.

14.3 For further information please contact GBS Data Protection Officer on dpa@globalbanking.ac.uk or refer to your line manager or Head of Department for reporting.

14.2

safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach**.**

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

Staff: all employees, workers, contractors, agency workers, consultants, directors, members, agency staff, temporary staff, work experience and volunteers and others.

ANNEX 2- GBS Data Breach Incident Report Form

DPO/INVESTIGATOR DETAILS:			
Name:		**Position:**	
Date:		**Time:**	
Tel:		**Email:**	

INCIDENT INFORMATION:	
Date/Time or period of Breach:	
Description & Nature of Breach:	
Type of Breach:	
Categories of Data Subjects Affected:	
Categories of Personal Data Records Concerned:	
No. of Data Subjects Affected:	
No. of Records Involved:	

IMMEDIATE ACTION TAKEN TO CONTAIN/MITIGATE BREACH:

ANNEX 3- GBS Data Breach Incident Report Flowchart