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
Oversight Committee	Executive Board
Policy lead (Staff member accountable)	Managing Director
Approved by	Executive Board
Approval date	February 2022
Date effective from	February 2022
Date of next review	February 2025
Version	1.0

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 Support to Study Policy ▪ GBS Student Charter ▪ GBS IT Security Policy ▪ GBS Privacy Policy ▪ GBS Email Usage 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, *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 is obliged under Data Protection legislation (UK GDPR and Data Protection Act 2018) to have in place an institutional framework designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility. This policy sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents across GBS. This policy relates to all personal and special categories (sensitive) data held by GBS regardless of format.

1.3 This policy applies to all staff and students at GBS. This includes temporary, casual or agency staff and contractors, consultants, suppliers, and data processors working for, or on behalf of GBS.

2. Objectives

2.1 The objective of this policy is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

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.

2.4 To utilise information audits and risk assessments for mapping data and to reduce the risk of breaches.

2.5 To have adequate and effective risk management procedures for assessing any risks presented by processing personal information.

2.6 To ensure that any data breaches are reported to the correct regulatory bodies within the timeframes set out in any regulations, codes of practice or handbooks.

2.7 To use breach investigations and logs to assess the root cause of any breaches and to implement a full review to prevent further incidents from occurring.

2.8 To use the Data Breach Incident Report Form (Annex 2) for all data breaches, regardless of severity so that any patterns in causes can be identified and corrected.

2.9 To protect students', employees and third parties; including their information and identity.

2.10 To ensure that where applicable, the Data Protection Officer is involved in and notified about all data breaches and risk issues. To ensure that the Information Commissioner's Office is notified of any data breach (where applicable) with immediate effect and at the latest, within 72 hours of GBS having become aware of the breach.

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).
- Accessing any part of a database using someone else's password.
- 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.

- ‘blagging’ offences where information is obtained by deceiving the 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 context “leave” implies its physical transport to an external, and insecure 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 “leave”.

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 GBS’ 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 for the specific purpose of use and intention. If not held under 'lock and key', 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 cases, it could be the DPO).

5.3 The DPO and potentially the relevant manager(s) will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

5.4 The DPO and potentially the relevant manager(s) will establish who may need to be notified as part of the initial containment and will inform the police, where appropriate.

5.5 Advice from experts across GBS may be sought in resolving the incident promptly.

5.6 The DPO, in liaison with the relevant manager(s) will determine the suitable course of action to be taken to ensure a resolution to the incident.

6. Investigation and Risk Assessment

6.1 An annual risk assessment and proportionate revision shall occur within each academic year.

6.2 If, following such a risk analysis, an individual identifies an imperative to take sensitive data off campus (in any media form) they are not to do so without prior consultation from GBS IT Services who can offer a range of suitable encryption solutions for the data prior to its removal from campus. Failure to comply with this requirement will be considered a serious breach of this policy. A breach of the GBS ICT Policy could lead to disciplinary measures, including dismissal, of an GBS staff member.

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 Commissioner's Office any data breaches in certain instances. Therefore, all staff have been made aware of GBS responsibilities and we have developed strict internal reporting lines to ensure that data breaches falling within the notification criteria are identified and reported without delay.

7.2 If for any reason it is not possible to notify the Information Commissioner's Office of the breach within 72 hours, the notification will be made as soon as is feasible, accompanied by reasons for any delay. Where a breach is assessed by the DPO and deemed to be unlikely to result in a risk to the rights and freedoms of natural persons, we reserve the right not to inform the Information Commissioner's Office in accordance with Article 33 of the UK GDPR.

7.3 The DPO, in consultation with relevant colleagues will establish whether the Information Commissioner's Office will need to be notified of the breach, and if so, notify them within 72 hours of becoming aware of the breach, where feasible.

7.4 Every incident will be assessed on a case-by-case basis; however, the following will need to be considered:

- Whether the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms under Data Protection legislation.
- Whether notification would assist the individual(s) affected (e.g., could they act on the information to mitigate risks?).
- Whether notification would help prevent the unauthorised or unlawful use of personal data.
- Whether there are any legal / contractual notification requirements.
- the dangers of over notifying. Not every incident warrants a notification and over notification may cause disproportionate enquiries and work.

7.5 The DPO must consider notifying third parties such as the police, insurers, banks or credit card companies, and trade unions. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

7.6 The DPO will consider whether the Marketing and Communications should be informed regarding a press release and to be ready to handle any incoming press enquiries.

7.7 A record will be kept of any personal data breach, regardless of whether notification was required.

8. Data Subject Notification

8.1 Individuals whose personal data has been affected by the incident, and where it has been considered likely to result in a high risk of adversely affecting that individual's rights and freedoms, will be informed without undue delay. The notification to the Data Subject shall include:

- A description of how and when the breach occurred, and the data involved.

- Specific and clear advice will be given on what they can do to protect themselves and include what action has already been taken to mitigate the risks.
- Individuals will also be provided with a way in which they can contact GBS for further information or to ask questions on what has occurred.

8.2 GBS reserves the right not to inform the data subject of any personal data breach where we have implemented the appropriate technical and organisational measures which render the data unintelligible to any person who is not authorised to access it (i.e., encryption, data masking etc) or where we have taken subsequent measures which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise.

8.3 If informing the data subject of the breach involves disproportionate effort, we reserve the right to instead make a public communication whereby the data subject(s) are informed in an equally effective manner.

9. Evaluation and response

9.1 Once the initial incident is contained, the DPO will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

9.2 Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring. The review will consider:

- Where and how personal data is held and where and how it is stored.
- Where the biggest risks lie including identifying potential weak points within existing security measures.
- Whether methods of transmission are secure, sharing minimum amount of data necessary.
- Staff awareness.
- Implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security.

9.3 If deemed necessary, a report recommending any changes to systems, policies and procedures will be considered by the Executive Board.

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. Data Protection Training & The DPO

14.1 GBS will ensure that all staff are provided with the time, resources, and support to learn, understand, and implement all procedures within this document, as well as understanding their responsibilities and the breach incident reporting lines.

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.

15. Alternative Format

15.1 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:

- **Name:** Welfare Management Team
- **Position:** Welfare Officer/Manager
- **Email:** welfare@globalbanking.ac.uk

ANNEX 1- Glossary

Data Controller: the person or organisation that determines when, why and how to process Personal Data.

Risk Assessment: A process for identifying and evaluating risks, either to people's rights and freedoms, or the risk of adverse events to a computer system.

Unauthorised: Without a legitimate right.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

United Kingdom General Data Protection Regulation (UK GDPR): The United Kingdom General Data Protection Regulation ((EU) 2016/679). Personal Data is subject to the legal safeguards specified in the GDPR.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access.

Data Protection Officer: A Data Protection Officer ensures that GBS processes the personal data of its staff, students or any other individuals (also referred to as data subjects) in compliance with the applicable data protection rules.

Information Commissioner's Office ("ICO"): ICO is the independent regulatory office in charge of upholding information rights in the interest of the public. The organisation covers the Data Protection Act and advises businesses on how to comply with UK GDPR and therefore requires every data controller who is processing personal information to register with the ICO.

Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational 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.

Student: a person who is studying at GBS or other place of higher education to attain a particular qualification to help enter a particular profession.

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:

Staff Involved in Breach:	
Procedures involved in Breach:	
Third Parties involved in Breach:	

BREACH NOTIFICATIONS:	
Was the Information Commissioner's Office Authority Notified?	**YES/NO**
If Yes, was this within 72 hours?	**YES/NO/N/A**
If no to the above, provide reason(s) for delay…	

Was the below information provided *(if applicable)*	**YES**	**NO**
A description of the nature of the personal data breach		
The categories and approximate number of data subjects affected		
The categories and approximate number of personal data records concerned		
The name and contact details of the Data Protection Officer and/or any other relevant point of contact (for obtaining further information)		
A description of the likely consequences of the personal data breach		
A description of the measures taken or proposed to be taken to address the personal data breach (including measures to mitigate its possible adverse effects)		
Was Notification provided to the Data Subject?		**YES/NO/N/A**

INVESTIGATION INFORMATION & OUTCOME ACTIONS:
Details of Incident Investigation:

Procedure(s) Revised due to Breach:
Staff Training Provided *(If applicable)*
DETAILS OF ACTIONS TAKEN AND INVESTIGATON OUTCOMES:
HAVE THE MITIGATING ACTIONS PREVENTED THE BREACH FROM OCCURING AGAIN? *(Describe)*

WERE APPROPRIATE TECHNICAL MEASURES IN PLACE?	**YES/NO/N/A**
If yes to the above, describe measures…	

GDPR Rep./Manager Signature …… Date: ……..
Data Protection Officer Signature ……... Date: ……

ANNEX 3- GBS Data Breach Incident Report Flowchart