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

Contents

1. Introduction and Scope 4
2. Objectives 4
3. Types of Breach 5
4. Reporting an Incident 8
5. Containment and Recovery 9
6. Investigation and Risk Assessment 9
7. Breach Notifications 10
8. Data Subject Notification 11
9. Evaluation and response 12
10. Record Keeping 13
11. Policy Review 13
12. Data Protection Policy Breach 13
13. Criminal Offence 13
14. Data Protection Training & The DPO 14
15. Alternative Format 14

ANNEX 1- Glossary 15
ANNEX 2- GBS Data Breach Incident Report Form 17
ANNEX 3- GBS Data Breach Incident Report Flowchart 20

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

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

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 neve Tmsf1 0 0 2[ib)-2(iliti)-2(es)-3( )-9iD(pe

locked down within servers, intranet, and cloud services with password protections as a minimum layer of security.

3.10

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 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

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 bece with (95.32595.32 841.92 reW*nt(tak)-4(es)-3( )

14. Data Protection Training & The DPO

14.1

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 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:	
[redacted]	

[redacted]

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**

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		

Procedure(s) Revised due to Breach:
Staff Training Provided *(If applicable)*
DETAILS OF ACTIONS TAKEN AND INVESTIGATON OUTCOMES:

ANNEX 3- GBS Data Breach Incident Report Flowchart