Global Banking School
+44 (0) 207 539 3548
info@globalbanking.ac.uk

Document title	GBS Data Protection Policy
Oversight Committee	Executive Board
Policy lead (Staff member accountable)	Managing Director
Approved by	Executive Board
Approval date	September 2019
Date effective from	September 2019
Date of next review	February 2025
Version	1.0

Related policies
▪ GBS Student Charter ▪ GBS Student Code of Conduct ▪ GBS Academic Good Practice and Academic Misconduct Policy and Procedure ▪ GBS Student Complaints Policy and Procedure ▪ GBS Academic Appeals Policy ▪ GBS Student Protection Plan ▪ GBS Student Disciplinary Policy ▪ GBS Equality and Diversity Policy ▪ GBS Social Media Policy ▪ GBS Safeguarding and Prevent Policy ▪ GBS Staff Disciplinary Policy ▪ GBS Grievance Policy ▪ GBS Staff Complaints Policy and Procedure
External Reference
▪ Information Commissioner's Office Accessed online at: https://ico.org.uk/ ▪ UK Public General Acts, *Equality Act 2010* Accessed online at: https://www.legislation.gov.uk/ukpga/2010/15/contents ▪ UK Public General Acts, *Data Protection Act 2018* Accessed online at: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Global Banking School Data Protection Policy

1.

Protection Act 2018 and UK GDPR. Please refer to each of our Partner Institutions specifically for further information on their data protection guidelines.

1.5 For any queries regarding

dpa@globalbanking.ac.uk to arrange additional training. GBS will regularly test our systems and processes to monitor compliance. For Data Protection purposes and compliance matters, please contact dpa@globalbanking.ac.uk.

5. Role and Responsibilities

5.1 Global Banking School 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 GDPR and DPA (2018). Roles and responsibilities include:

- **GBS Senior Management Team:** Responsible for ensuring that their staff are made aware of this policy and that breaches are dealt with appropriately and developing and encouraging good information handling practices within their areas of responsibility.

- **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.

- **Data Protection Officer:** DPO is responsible for advising Global Banking School on its obligations, monitoring compliance, assisting with Data Protection Impact Assessments (DPIAs) and liaising with the Information Commissioner's Office. The DPO is also responsible for ensuring that GBS processes the personal information of its staff, students, customers, providers, and partners in compliance with the applicable data protection rules. Any issues related to Data Protection and compliance issues, please contact dpa@globalbanking.ac.uk.

- **GBS**

ICT Department: ICT are responsible for ensuring that advice and guidance on technical specifications and technical security measures are made available to staff such as the GBS ICT Policy.

a) as set out in the applicable Transparency Notice

b) protecting and promoting GBS legitimate interests and objectives and

c) to fulfil the GBS contractual and other legal obligations.

7.4 *Use of Personal Data*- If you want to do something with Personal Data that is not

10.4 If you have any questions about your processing of these categories of Critical GBS Personal Data please speak to GBS Data Protection Officer who will be happy to assist you. Any issues relating to compliance please use dpa@globalbanking.ac.uk.

11. Processing Personal Data: Responsibilities of Staff

11.1 *Personal Data must only be processed for limited purposes and in an appropriate way. What does this mean in practice?*

11.2 For example, if employees are told that they will be photographed for GBS website or intranet, you should not use those photographs for another purpose (e.g., GBS marketing material or social media accounts).

11.3 When you are designing a new process or procedure you must take account of the Privacy by Design requirements which include undertaking an appropriate Data Protection Impact Assessment. When you are planning your changes, please speak to GBS DPO for advice and assistance.

11.4 *Personal Data held must be adequate and relevant for the purpose. What does this mean in practice?*

11.5 This means not making decisions based on incomplete data. For example,

12.3 **DO** encrypt emails which contain Critical GBS Personal Data. For example, encryption should be used when sending details of an employee's ill health to external advisers or insurers; or payroll details which are likely to contain several pieces of Critical GBS Personal Data including details of trade union membership to the payroll provider.

12.4 **DO** make sure that you have permission from your line manager or GBS DPO to share Personal Data on GBS website.

12.5 **DO** be aware of "blagging". This is the use of deceit to obtain Personal Data from people or organisations. You should seek advice from GBS DPO where you are suspicious as to why the information is being requested or if you are unsure of the identity of the requester (e.g., -7(e)-11( )51(6hl2 reW*nBT/F11 07(e)-[t)5(o)-111(n)-ce)-11( )5(

they are away, using your personal mobile device without GBS consent.

15. Individuals' rights in their Personal Data

15.1 The UK GDPR and DPA 2018 provides you with Individual's rights**:** People have various rights to their information. You must be able to recognise when someone is exercising their rights so that you can refer the matter to GBS DPO. Please let GBS DPO know if anyone (either for themselves or on behalf of another person, such as a solicitor):

- **The right of access/to be informed**-wants to know what information GBS holds about them.
- **The right to withdraw** -asks to withdraw any consent that they have given to use their information.
- **The right to erasure**-

16.2 Form of request: Subject Access Requests do not have to be labelled as such and do not even have to mention data protection. For example, an email which simply states "Please send me copies of all emails you hold about me" is a valid Subject Access Request. You must always immediately let GBS DPO know when you receive any such requests.

16.3 Please see APPENDIX D for an example of a Subject Access Request. Please note, th.3

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

18. Criminal Offence

18.1 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

APPENDIX A
Glossary

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Data Controller:

erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

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, contra

APPENDIX C
Staff Guide on Sharing Personal Data: Dos and

All GBS staff must ensure that the requirements of the UK Data Protection Act 2018 are observed at all times. Guidance is given below concerning what you should do and what you should not do in this respect. Please read this guidance carefully and try to ensure you adhere to guidance at all times. If you have any questions or areas for clarification please contact GBS Academic Standards and Quality Office (ASQO), asqo@globalbanking.ac.uk, in the first instance. A folder on SharePoint GBS Internal Data Protection Policies and Procedures' has been created for you to access. In the first instance this guidance is available there.

DO share Personal Data strictly on a need-to-know basis - think about why it is necessary to share data outside of GBS - if in doubt - always ask your line manager.

DO encrypt emails which contain Critical GBS Personal Data. For example, encryption should be used when sending details of an employee's ill health to external advisers or insurers; or payroll details which are likely to contain several pieces of Critical GBS Personal Data including

Please note, the above subject access request example was obtained from the ICO website.