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

GBS Data Protection Policy

Document title	GBS Data Classification and Handling 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

Contents

Global Banking School Data Protection Policy

1. Introduction and Scope

1.1 Global Banking School (GBS) needs to collect, store and process personal data about its staff, students, and other individuals it has dealings with, to carry out our functions and activities. GBS is a controller for most of the personal data it processes and is committed to full compliance with the applicable data protection legislation including The Data Protection Act 2018 and the United Kingdom General Data Protection Regulation (UK GDPR). This policy sets out how GBS ("we", "our", "us") handle the personal data of our staff, clients, suppliers, partners, employees, workers and other third parties.

1.2 To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The policy applies to all staff and students of GBS, and the handling of all personal data processed by GBS. Mandatory training will be provided to staff to assist them in meeting their obligations under this policy. As a matter of good practice, other agencies and individuals working with GBS, and who have access to personal information, will be expected to have read and comply with this policy. It is expected that partners and services who deal with external agencies will take responsibility for ensuring that such agencies sign a contract agreeing to abide by this policy.

1.3 This policy is about your obligations under the data protection legislation. Data protection is about regulating the way that GBS uses and stores information about identifiable people (Personal Data). *Please refer to Appendix B for examples of the types of data that can constitute 'Personal Data'.* It also gives people various rights regarding their data - such as the right to access the personal data that GBS holds on them. We try to avoid using legalese or jargon in this policy; however, certain words and phrases have particular meanings under data protection legislation. *Please* refer to the Glossary at Appendix A for definitions used in this policy.

1.4 If you are involved in study arrangements with any of GBS Collaborative Partner Institutions, please note that all our partners are also data controllers and are

responsible for the same regulations as GBS and must comply with Data 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 the Data Protection Policy and any issues relating to compliance and data protection matters please contact our Data Protection Officer on E: dpa@globalbanking.ac.uk.

2. Data Protection Background

2.1 The purpose of the UK GDPR and Data Protection Act 2018 is to protect the rights and privacy of living individuals and to ensure that personal data and information is not processed without their knowledge and is processed with a clear legal basis. During the course of our business we will collect, store and process personal data about our staff, students, clients, suppliers and other third parties. We recognise that the correct and lawful treatment of this data will maintain confidence in GBS and will ensure that GBS operates successfully. This policy is aimed at all staff working at GBS (whether directly or indirectly), whether paid or unpaid, whatever their position, role, or responsibilities ('you'). You are obliged to comply with this policy when processing personal data on our behalf. Any breach of this policy could lead to disciplinary action.

3. Guidance and related policies

3.1 This policy is accompanied by the Staff Handbook and must be followed to achieve GBS policy objectives. Reference should also be made to the GBS Privacy Policy, GBS Data Subject Access Request Policy, GBS Records Management Policy, GBS ICT Policy, and GBS Equality and Diversity Policy. Information on other related policies is available from GBS Academic Standards and Quality Office (ASQO).

4. Staff Training and Audit

1.6 This policy may be amended by GBS at any time. GBS will ensure that all staff receive appropriate training to enable them to comply with this policy and Data Protection Law. Data Protection training is mandatory. Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with

them. Any individual who does not think they are sufficiently aware of Data Protection Law should contact Data Protection Officer on E: 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 Academic Standards And Quality Office (ASQO):** Responsible for monitoring and review of this policy and can be contacted on asqo@globalbanking.ac.uk.

- **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.

- **Line Managers:** Responsible for ensuring that their staff have completed all required training in Data Protection. Ensuring that activities requiring a Data Protection Impact Assessments (DPIA) are referred to the DPO. Ensuring that requests made under data subject rights are referred to GBS Academic Standards and Quality Office (ASQO) promptly and ensuring that suspected or actual compromises of personal data are reported immediately.

- **GBS Staff:** Responsible for complying with Data Protection Policy. Completing all required data protection training including refresher training as and when required. They must ensure that they are processing data in line with GBS policies and requirements. Staff will be required to sign and date a training acknowledgement form to confirm they have received the mandatory training on Data Protection and UKGDPR.

- **ALL GBS Members (staff and students)-**Responsible for ensuring that *any* personal data that they supply about themselves to GBS are accurate and up to date. All members of staff and students are advised to familiarise themselves with the appropriate GBS Privacy Policy. Any issues related to Data Protection and compliance issues, please contact dpa@globalbanking.ac.uk.

6. The Principles of Data Protection

6.1 We adhere to the principles relating to Processing of Personal Data set out in Chapter 2 Article 5 UK GDPR which provides us with the main responsibilities to ensure that personal data is:

(a) Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).

(b) Collected only for specified, explicit and legitimate purposes (Purpose Limitation).
(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation).
(d) Accurate and where necessary kept up to date (Accuracy).
(e) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation).
(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction, or damage (Security, Integrity and Confidentiality).
(g) Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).
(h) Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

6.2 Global Banking School as Data Controller shall be responsible for and must be able to demonstrate compliance with the data protection principles listed above and will implement appropriate technical and organisational measures to ensure compliance. (Accountability). For further information on our responsibilities, please see the ICO website.

7. Your obligations

7.1 Article 6 UK GDPR sets out the Lawfulness of processing: Personal Data must be processed fairly, lawfully and transparently. What does this mean in practice?

(a) "Processing" covers virtually everything which is done in relation to Personal Data, including using, disclosing, copying and storing Personal Data.
(b) People must be told what data is collected about them, what it is used for, and who it might be shared with, unless it is obvious. They must also be given other information, such as, what rights they have in their information, how long we keep it for and about their right to complain to the Information Commissioner's Office ("ICO").

7.2 This information is often provided in a document known as a Transparency Notice. Copies of GBS Transparency Notices can be obtained from the Data Protection Officer.

7.3 You must only process Personal Data for the following purposes:

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 on the above list, you must speak to Data Protection Officer (DPO). This is to make sure that GBS has a lawful reason for using the Personal Data. If you are using Personal Data in a way which you think an individual might think is unfair please speak to the Data Protection Officer (DPO).

8. Transfer outside the EU/EEA[1]

8.1 The UK has incorporated the GDPR into the withdrawal bill and pending an adequacy decision, the EU-UK Trade and Cooperation Agreement contains a bridging mechanism that allows the continued free flow of personal data from the EU/EEA to the UK until adequacy decisions come into effect, for up to six months. The UK GDPR requires Data Controllers to ensure that any Personal Data sent to any country outside the EU/EAA is afforded the same level of protection as in the EU.

8.2 Transfers outside the EU/EAA are only permitted in the following situations:

- The European Commission has issued a decision confirming the country receiving the Personal Data is provides an adequate level of protection.
- Appropriate safeguards are in place such as binding corporate rules or standard contractual clauses.
- The data subject has provided explicit consent to the proposed transfer having been informed of all the risks.

[1] *Please note these are subject to change and will be reviewed according to ICO guidance.*

8.3 The transfer is necessary for one of the reasons set out in the UK GDPR including:

- The performance of a contract.
- Reasons of public interest.
- For the establishment or defence of legal claims.
- In the Vital Interests of a Data Subject.

8.4 Where transfers are being made out of the EU/EEA, advice should be sought from GBS Academic Standards and Quality Office (ASQO). For more information on transfers outside the EU/EEA, please visit ICO website.

9. Consent

9.1 We may sometimes rely on the consent of the individual to use their Personal Data. This consent must meet certain requirements and therefore you should speak to GBS Data Protection Officer (DPO). if you think that you may need to obtain consent. Consent is required for certain mail-outs and marketing by electronic means, please check with the DPO before sending mail-outs to clients.

10. Personal Data at work

10.1 In order for you to do your job, you will need to collect, use and create Personal Data. Virtually anything that relates to a living person will include Personal Data. Examples of places where Personal Data might be found are:

(a) on a computer database
(b) in a file, such as a personnel or client record
(c) in a register or contract of employment
(d) letters, attendance notes, meeting minutes and other documents or written records
(e) health records
(f) email correspondence
(g) work mobile telephones
(h) work tablets

10.2 Categories of Critical GBS Personal Data:

10.3 The following categories are referred to as Critical GBS Personal Data in this policy. You must be particularly careful when dealing with Critical GBS Personal Data which falls into any of the categories below:

(a) physical or mental health or condition

(b) racial or ethnic origin

(c) religious beliefs or other beliefs of a similar nature

(d) information relating to actual or alleged criminal activity; and

(e) genetic or biometric information.

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, when undertaking an employee's performance review, you must make sure you are using all the relevant and most up to date information about the employee.

11.6 *Personal Data must not be excessive or unnecessary. What does this mean in practice?*

11.7 Personal Data must not be processed in a way that is excessive or unnecessary. For example, you should only collect information about an employee's family when it is necessary in relation to work, such as to ensure GBS is aware of an employee's childcare arrangements to assist with flexible working.

11.8 *Personal Data that you hold must be accurate. What does this mean in practice?*

11.9 You must ensure that Personal Data is complete and kept up to date. For example, if a students, staffs, or client's contact details have changed, you should update GBS information management system.

11.10 *Personal Data must not be kept longer than necessary. What does this this mean in practice?*

11.11 GBS holds different types of data for different amounts of time. This applies to both paper and electronic documents. You must be particularly careful when you are deleting data. Please speak with GBS DPO for guidance on the retention periods and secure deletion.

11.12 *Personal Data must be kept secure.* You must comply with the following GBS policies and guidance relating to the handling of Personal Data, which can be found in the Staff Handbook:

(a) CCTV & security
(b) Monitoring
(c) Email and internet use
(d) Social media
(e) Anti-corruption & bribery; and
(f) Screening

11.13 *Personal Data must not be transferred outside the EEA without adequate protection. What does this mean in practice?*

11.14 If you need to transfer personal data outside the EEA please contact GBS DPO. For example, if you are arranging a GBS trip to a country outside the EEA or working with a client based outside the EEA.

12. Sharing Personal Data outside GBS - Dos and Don’ts

12.1 Please review the following dos and don'ts:

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

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., if a request has come from an existing client but using a different email address).

12.6 **DO** be aware of phishing. Phishing is a way of making something (such as an email or a letter) appear as if it has come from a trusted source. This is a method used by fraudsters to access valuable personal details, such as usernames and passwords. Don't reply to email, text, or pop-up messages that ask for personal or financial information or click on any links in an email from someone that you don't recognise. Report all concerns about phishing to the IT department.

12.7 **DO NOT** disclose Personal Data to the Police or other statutory agencies such as HMRC or a Local Authority without permission from GBS DPO.

12.8 **DO NOT** disclose Personal Data to contractors without permission from GBS DPO. This includes, for example, sharing Personal Data with an external

marketing team to carry out a marketing campaign. *For more examples on Staff Do's and Don'ts please see APPENDIX C.*

13. Processing Personal Data: Responsibilities of Students

13.1 This policy applies to students where they are collecting personal information on behalf of GBS, for example conducting research and collecting personal data as part of their role as Student Representative. In connection with students' academic studies/research if required or necessary, all GBS students have the following responsibilities:

- To notify an appropriate member of staff, usually their tutor, if they intend to process information about identifiable individuals as part of their academic studies/research.

- To only process Personal Data for use in academic studies/research which has been expressly authorised by a member of staff.

- To comply with any regulations or requirements implemented by GBS or by a member of GBS staff in order to facilitate compliance with Data Protection Law; and

- To have reference and to adhere to GBS Data Protection Policy, Procedures and Guidelines at all times.

13.2 In relation to any activities not specifically authorised by GBS, students processing Personal Data are responsible for their own compliance with Data Protection Law.

14. Sharing Personal Data within GBS

14.1 This section applies when Personal Data is shared within GBS. Personal Data must only be shared within GBS on a "need to know" basis.

14.2 Client files should be locked down to the Staff who need to access the information for business purposes and wider access granted only to persons with appropriate authority. If you are unsure whether a person has appropriate authority speak to GBS DPO.

14.3 Examples of internal sharing which are **likely** to comply with the UK GDPR:

(a) liaising with Human Resources Management with CEO and Senior Managers in respect of employees' pay reviews.

14.4 Examples of internal sharing which are **unlikely** to comply with the UK GDPR:

(b) recording an interview or telephone call without the other person knowing, leaving handover notes on a colleague's desk while 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**-wants GBS to delete any information.
- **The right to rectification**-asks GBS to correct or change information (unless this is a routine updating of information such as contact details, which falls within your role and authorised access).
- **The right to data portability**-asks for electronic information which they provided to GBS to be transferred back to them or to another organisation.
- **The right to restrict processing**- wants GBS to stop using their information for direct marketing purposes. Direct marketing has a broad meaning for data protection purposes and might include communications such as GBS; or
- **The right to object**- objects to how GBS is using their information or wants the GBS to stop using their information in a particular way, for example, if they are not happy that information has been shared with a third party.

15.2 For more information on the above UK GDPR rights, please revert to the ICO website.

16. Requests for Personal Data (Subject Access Requests)

16.1 One of the most commonly exercised rights is the right to make a Subject Access Request. Under this right people are entitled to request a copy of the Personal Data which GBS holds about them and to certain supplemental information.

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, the subject access request image was obtained from the ICO website.

16.4 Receiving a Subject Access Request is a serious matter for GBS and involves complex legal rights. Staff must never respond to a subject access request themselves unless authorised to do so.

16.5 Disclosure: When a Subject Access Request is made, GBS must disclose all of that person's Personal Data to them which falls within the scope of the request - there are only very limited exceptions. There is no exemption for embarrassing information - so think carefully when writing letters and emails as they could be disclosed following a Subject Access Request. However, this should not deter you from recording and passing on information where this is appropriate to fulfil your professional duties, particularly in relation to money laundering or fraud prevention.

16.6 Further guidance on making a ‘subject access request’ and the process can be found under GBS Data Subject Access Request Policy.

17. Data Protection Policy Breach

17.1 GBS takes compliance with the Data Protection policy very seriously, therefore a breach of this policy may be treated as misconduct and could result in disciplinary action and in serious cases, may lead to dismissal. If staff or students are found to be in breach of this policy, GBS has the authority to revoke your access to the Schools 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 the School.
- 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 and criminal sanctions for the individual and the school, which can lead to:

- Significant legal and financial consequences. Monetary penalties of the Information Commissioners Office can reach up to 20 million euros or 4% of turnover.
- Individual civil action for breaches of data protection can also be taken by individuals or third-party organisations where there is a failure to meet contractual obligations to hold data securely.

19. Alternative Format

19.1 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

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: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Data Controller of all Personal Data relating to GBS Personnel and Personal Data used in our business for our own commercial purposes.

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.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

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. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Data Protection Impact Assessments (DPIA): A Data Protection Impact Assessment (DPIA) is a process to help companies identify and minimise the data protection risks of a project. This is carried out for processing that is likely to result in a *high risk* to individuals in regard to their personal data.

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**.**

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with UKGDPR.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of

operations on the data including organising, amending, retrieving, using, disclosing, 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, 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.

Transparency Notices (also referred to as Fair Processing Notices) or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when GBS collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee Transparency Notices or the website privacy policy) or they may be stand-alone, one-time privacy statements covering Processing related to a specific purpose.

APPENDIX B
Personal data

The following are examples of the types of data that can constitute 'Personal data':

***Name**

***Data of Birth/Age**

***Postal Address(es) (to include postcodes)**

***Contact telephone(s)**

***Email address(es)**

***Unique Identifiers (to include Student ID numbers, Staff ID numbers, Passport numbers, NHS**

numbers, National Insurance numbers, Unique applicant ID numbers, vehicle reg, driving licence numbers)

***Images of individuals, including CCTV, photos.**

***Location Data (to include any GPS tracking data)**

***Online Identifiers (to include IP address data)**

***Economic/financial data (relating to an identifiable individual)**

***Educational records including but not limited to records held by GBS/other education providers.**

***Counselling records**

***Pastoral records, including Extenuating Circumstances Forms**

***Disciplinary records/Training records**

***Employment records to include CV's, references.**

***Nationality/Domicile**

***Ethnicity**

***Mental Health (status, medical records conditions, to include disability)**

***Physical Health (status, medical records conditions, to include disability)**

***Dietary requirements**

***Sexual Orientation/Sexual life**

***Genetic Data (to include DNA data)**

***Biometric data (such as facial image or fingerprint data)**

***Political opinions/Trade Union membership**

***Religious or philosophical beliefs**

***Criminal Convictions and offences (to include alleged offences and convictions)**

APPENDIX C
Staff Guide on Sharing Personal Data: Dos and Don'ts

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's

- **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 details of trade union membership to the payroll provider.
- **DO** make sure that you have permission from your line manager or GBS DPO to share Personal Data on GBS website.
- **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., if a request has come from an existing client but using a different email address).
- **DO** be aware of phishing. Phishing is a way of making something (such as an email or a letter) appear as if it has come from a trusted source. This is a method used by fraudsters to access valuable personal details, such as usernames and passwords.
- **DO** shred personal data if in paper form and arrange certified confidential waste disposal for large amounts of personal data as and when approved and required by GBS.
- **DO** keep your username and passwords secure and do not share these amongst colleagues
- **DO** report any data breaches immediately and undertake regular training on Data Protection and UK GDPR
- **DO** verify an individual before handing over personal data, whether its by phone, email or face to face.
- **DO** be vigilant with emails and attachments
- **DO** familiarise yourself with all GBS policies and procedures
- **DO** log out when not using digital services especially GBS internal emails and software such as Moodle, teams, Microsoft Outlook.
- **DO** audit the data you are using on a day-to-day basis within the scope of UK GDPR.

DONT'S

- **DO NOT** leave any personal information lying around at home or in the office
- **DO NOT** give your username or password to anyone
- **DO NOT** dispose of personal data in regular bins or recycling if it has not been shredded or destroyed
- **DO NOT** open emails or attachments from unknown sources
- **DO NOT** duplicate personal data unnecessarily e.g. printing it out
- **DO NOT** download GBS data onto personal devices unless authorised to do so
- **DO NOT** leave your computer logged in if you can access personal data from it i.e. student information or sensitive information
- **DO NOT** store your passwords in browsers
- **DO NOT** log into public wi-fi or unsecured networks whilst working with personal data
- **DO NOT** provide access to personal data unless it is necessary and lawful
- **DO NOT** disclose Personal Data to the Police or other statutory agencies such as HMRC or a Local Authority without permission from GBS DPO.
- **DO NOT** disclose Personal Data to contractors without permission from GBS DPO This includes, for example, sharing Personal Data with an external marketing team to carry out a marketing campaign.
- **DO NOT** put actual student names in emails, instead use code such as Student A, Student B, Student C so on and so forth.
- **DO NOT** circulate emails to others with emails addresses on, especially if private email addresses of staff or student or external to GBS.
- **DO NOT** keep inaccurate data as this is a breach of data protection legislation
- **DO NOT** assume that data protection doesn't matter – **IT DOES**
- **DO NOT** reply to email, text, or pop-up messages that ask for personal or financial information or click on any links in an email from someone that you don't recognise. Report all concerns about phishing to the IT department.

APPENDIX D
Example of a Subject Access Request

[Name and address of the organisation]

[Your name and full postal address]

[Your contact number]

[Your email address]

[The date]

Dear Sir or Madam

Subject access request

[Include your full name and other relevant details to help identify you].

Please supply the personal data you hold about me, which I am entitled to receive under data protection law, held in:

[Give specific details of where to search for the personal data you want, for example:

- my personnel file;
- emails between 'person A' and 'person B' (from 1 June 2017 to 1 Sept 2017)
- my medical records (between 2014 and 2017) held by 'Dr C' at 'hospital D';
- the CCTV camera situated at ('location E') on 23 May 2017 between 11am and 5pm; and
- financial statements (between 2013 and 2017) held in account number xxxxx.]

If you need any more information, please let me know as soon as possible.

[If relevant, state whether you would prefer to receive the data in a particular electronic format, or printed out].

It may be helpful for you to know that data protection law requires you to respond to a request for personal data within one calendar month.

If you do not normally deal with these requests, please pass this letter to your data protection officer or relevant staff member.

If you need advice on dealing with this request, the Information Commissioner's Office can assist you. Its website is ico.org.uk, or it can be contacted on 0303 123 1113.

Yours faithfully

[Signature]

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