Document title	GBS Data Protection Policy
Version	V1.1
Approved by (Oversight Committee)	Board of Directors
Policy lead (Staff member accountable)	Data Protection Officer
Date of original approval	September 2019
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	December 2026

Related policies
GBS Student Charter
GBS Student Code of Conduct
GBS Academic Good Practice and Academic Conduct 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 Policy
GBS Staff Disciplinary Policy
GBS Grievance Policy
GBS Staff Complaints Policy and Procedure
External Reference
Information Commissioner's Office Accessed online at: https:// 46/Las:// 46/Las:/

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

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.

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

The performance of a contract.

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

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)

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)(f)

12. Sharing Personal Data outside GBS - D

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 wit

(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

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 staff0.5 696.94 Tm0 g0 G[ )]TE

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

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

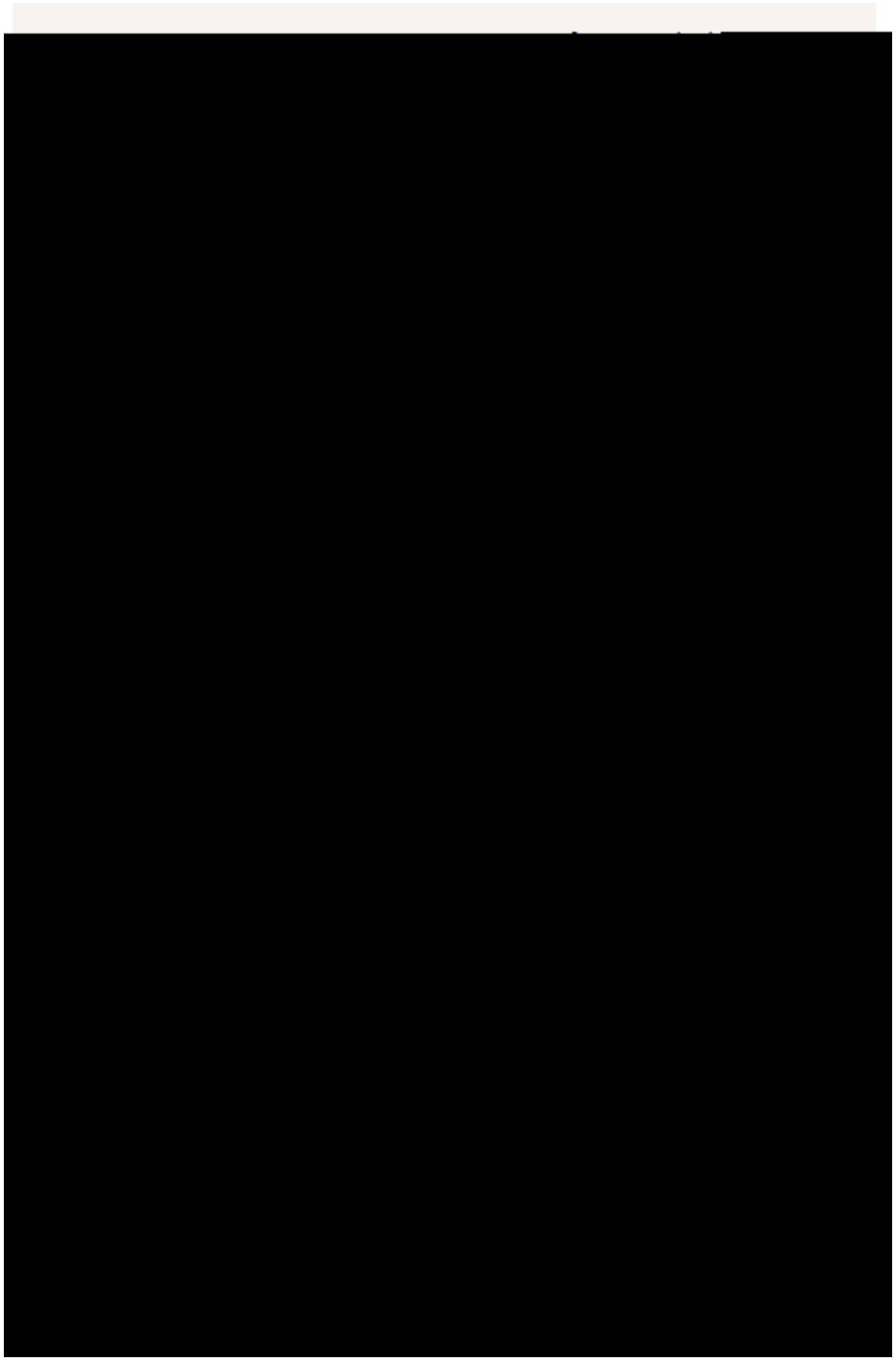
DO NOT leave any personal information lying around at home or in the office

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



Please note, the above subject access request example was obtained from the [ICO website](#).