



Global Banking School
+44 (0) 207 539 3548

info@globalbanking.ac.uk

www.globalbanking.ac.uk

891 Greenford Road, London
UB6 0HE

GBS Data Subject Access Request (DSAR) Policy

©2022 Global Banking School

Version Control

Document title	GBS Data Subject Access Request (DSAR) Policy
Version	V2.1
Approved by (Oversight Committee)	Board of Directors
Policy lead (Staff member accountable)	Managing Director
Date of original approval	February 2022
Date of last review	December 2024

Changes made at the last review:

Global Banking School Data Subject Access Request (DSAR) Policy

1. Purpose 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. The Data Protection Act 2018 (DPA) and the United Kingdom General Data Protection Regulation (UK GDPR) gives individuals rights of access to their personal records held by GBS, subject to certain exemptions. This is known as a 'Subject Access Request' (SAR).

1.2 GBS regards the Data Protection Act as an important mechanism in achieving an honest, safe, and open relationship with its students and staff. Requests may be received from members of staff, students, members of the public and any other individual who GBS has had dealings with and holds data. This policy explains how GBS will fulfil its obligations under the Act and provides a guide to staff in dealing with subject access requests that may be received.

2. Role and Responsibilities

2.1 GBS is registered with the Information Commissioner's Office as a data controller. Details of the school's registration are published on the Information Commissioner's 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:

2.1.1 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.

2.1.2 Data Protection Officer: DPO is responsible for advising GBS 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

excessive” before relying on this exemption, particularly as it is likely to be a high threshold to satisfy.

4.4 GBS in some circumstances may extend the time limit by a further two months if the request is complex or *if* several requests are made from the same individual.

5. Verification

5.1 Staff must ensure a request has been received in writing where a data subject is asking for sufficiently well-defined personal data held by GBS. The Data Protection Act permits and encourages us to clarify with the requestor what information they need.

5.2 Data subjects must supply their address and valid evidence to prove their identity. GBS accepts the following forms of identification:

- Current UK/EEA Passport (valid)
- UK Photocard Driving Licence (Full or Provisional, valid)
- Firearms Licence / Shotgun Certificate (valid)
- EEA National Identity Card (valid)
- Full UK Paper Driving Licence (valid)
- State Benefits Entitlement Document (past 12 months)
- State Pension Entitlement Document (past 12 months)
- HMRC Tax Credit Document (past 12 months)
- Local Authority Benefit Document (past 12 months)
- State/Local Authority Educational Grant Document or SLC approved documentation (past 12 months)
- HMRC Tax Notification Document (past 12 months)
- Disabled Driver’s Pass
- Financial Statement issued by bank, building society or credit card company (past 3 months)
- Judiciary Document such as a Notice of Hearing, Summons or Court Order (past 3 months)
- Utility bill for supply of gas, electric, water or telephone landline (past 3 months)
- Most recent Mortgage Statement (past 12 months)
- Most recent Council Tax Bill/Demand or Statement (past 3 months)
- Current Council Rent Card (past 3 months)
- Current Council Tenancy Agreement (past 12 months)

Building Society Passbook which shows a transaction in the last 3 months and your address.

6. Processing a Subject Access Request (SAR)

6.1 Following receipt of a subject access request, and provided that there is sufficient information to process the request, an entry should be made within GBS' subject access logbook and must include:

The date of receipt

The data subject's name

The name and address of requester (if different)

The type of data required (e.g., Student Record, Personnel Record)

The planned date for supplying the information (not more than one calendar month from the request date).

6.2 Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the date of entry in the log will be the date on which sufficient information has been provided. (Please refer to Annex 3 to view GBS Subject Access Request Flow Chart).

6.3 By ensuring that the Human Resources department has logged the request, we can ensure that we respond within the statutory timescales. As the time for responding to a request does not stop during the periods when GBS is closed for the holidays. GBS will attempt to mitigate any impact this may have on the rights of data subjects to request access to their data by implementing any necessary measures.

6.4 When responding to a complaint, we must advise the requestor that they may complain to the ICO if they remain unhappy with the outcome.

6.5 If a subject access request is related or may be connected to a disciplinary or grievance for an employee, individual or student, GBS staff should ensure that the broader context is considered when responding to a request and seek advice if required on managing the broader issue and the response to the request.

6.6 Depending on the degree to which information is organised and structured, staff

Emails (including archived emails and those that have been deleted but are still recoverable).

Word documents, spreadsheets, databases, systems.

CCTV, removable media (for example, memory sticks, floppy disks, CDs)

Tape recordings, paper records in relevant filing systems etc.

6.7 Staff must not withhold information because they believe it will be misunderstood; instead, they should provide an explanation with the information. Staff must provide the information in an “intelligible form”, which includes explaining any codes, acronyms, and complex terms. The information must be supplied in a permanent form except where the person agrees or where it is impossible or would involve undue e

information, depending on the circumstances. GBS can also refuse to comply with a SAR if it is 'manifestly unfounded or manifestly excessive'. If GBS refuses to comply with a request, the individual must be informed of:

The reasons why.

Their right to make a complaint to the ICO or another supervisory authority; and

Their ability to seek to enforce this right through the courts.

7.4 If a request involves information about other individuals, GBS will consider whether it is possible to comply with the request without disclosing information that identifies another individual. If this is not possible, GBS does not have to comply with the request except where the other individual consents to the disclosure or it is reasonable to comply with the request without that individual's consent.

7.5 Data on a deceased person is confidential however it is not covered by the Data Protection Act but instead by the Freedom of Information Act. In deciding whether to allow access to an individual requesting information in relation to a deceased person staff will need to consider any responsibility of confidentiality to that deceased person. Staff should also consider the rights of the data subject under the Human Rights Act, Article 8

- f The existence of any automated decision-making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

9. Related policies/Review

9.1 Reference should also be made to GBS Data Protection Policy, GBS Privacy Policy, GBS Records Management 0 1 84.48 629.98 Tm0 g0 G 0.0151 Tc(9.1)JTJETQ EMC /Span #MCID 4



Annex 1- Example of a Subject Access Request

Annex 2- Subject Access Request Form

It is not mandatory to use this form, however it will help us to give a timely and accurate response to your subject access request under data protection legislation. Please complete the table below and return the form by email (or post) to Human Resources at GBS.

Date	
Title (Mr, Ms, etc.)	
Surname	



Information Commissioner's Office ("ICO") ICO is the independent regulatory office in charge of upholding information rights in the interest of the public.

Breach any act or omission that compromises the security, confidentiality, integrity or availability of personal data.

