

GBS Data Subject Access Request Policy

INTRODUCTION / OVERVIEW

1. The GDPR extends to all data subjects a right of access to their own personal data. This is known as a subject access request. A formal request from a data subject for information that a school holds about them must be made in writing. A school can invite a data subject to complete a form but you cannot insist that they do so. A subject access request can be made by anyone including students and members of the public.
2. It is important that all members of staff are able to recognise that any written request made by a person for their own information is likely to be a valid subject access request, even if the individual does not specifically use this phrase in their request or refer to the GDPR. In some cases, an individual may mistakenly refer to the “Freedom of Information Act” but this should not prevent the school from identifying the request as being made under the GDPR if appropriate. Some requests may be a combination of a subject access request for personal data under the GDPR and a request for information under the Freedom of Information Act 2000 (“FOIA”). Requests for information under the FOIA must be dealt with promptly and in any event within 20 school days
3. Any member of staff who receives a written request for their personal data must immediately forward it to the School Head of Compliance as the statutory time limit for responding under the GDPR is **one calendar month** from receipt. Under the Data Protection Act 1998, Data Controllers previously had 40 calendar days to respond to a request. The timescales for responding do not pause when the School is closed for holidays, unlike the FOIA.
4. A fee may no longer be charged to the individual for provision of this information (previously a fee of £10 could be charged under the Data Protection Act 1998). You must provide a copy of the information free of charge. However, you can charge a ‘reasonable fee’ when a request is “manifestly unfounded or excessive”, particularly if it is repetitive. It is advisable for the School to consult any guidance issued by the Information Commissioner’s Office (ICO) on what is deemed to be “manifestly unfounded or excessive” before relying on this exemption, particularly as it is likely to be a high threshold to satisfy. You may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that you can charge for all subsequent access requests. The fee must be based on the administrative cost of providing the information.
5. GBS may ask the Data Subject for reasonable identification so that they can satisfy themselves about the person’s identity before disclosing the information.

6. In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place. Certain information may be 3 exempt from disclosure so you will need to consider what exemptions apply and decide whether you can rely on them. In practice, this means that you may be entitled to withhold some documents entirely or you may need to redact parts of them. Care should be taken to ensure that documents are redacted properly. Please seek further advice or support if you are unsure which exemptions apply.

7. Requests from learners should be processed as a subject access request and would not normally be charged with a fee unless the administration was reasonably deemed “manifestly unfounded or excessive” by the GBS Managing Director or CEO.

8. Following receipt of a subject access request, and provided that there is sufficient information to process the request, an entry should be made in the School subject access log book, showing 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), and the planned date for supplying the information (not more than one calendar month from the request date). 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 date on which sufficient information has been provided.

9. In the context of a School sometimes a subject access request is normally wrapped up in a broader complaint or concern from a learner or may be connected to a disciplinary or grievance for an employee. GBS should therefore always ensure that the broader context is taken into account when responding to a request and seek advice if required on managing the broader issue and the response to the request.

Guidance for staff on responding to a subject access request

What must I do?

1. On receipt of a subject access request you must forward it immediately to the GBS Head of Compliance

2. We must correctly identify whether a request has been made / ensure that it is not being confused with the rights that people have to request information under the Freedom of Information Act 2000.

3. Any employee who receives a request to locate and supply information relating to a SAR must make a full exhaustive search of the records to which they have access.

4. All the information that has been requested must be provided unless an exemption can be applied.
5. We must respond within one calendar month after accepting the request as valid.
6. Subject Access Requests must be undertaken free of charge to the requestor
7. Line managers must ensure that the staff they manage are aware of and follow this guidance.
8. Where a requestor is not satisfied with a response to a SAR, the School must manage this in accordance with its complaints policy.

How must I do it?

1. We must ensure a request has been received in writing where a data subject is asking for sufficiently well-defined personal data held by the School relating to themselves.
2. The Act permits and encourages us to clarify with the requestor what information they need. They must supply their address and valid evidence to prove their identity. The School 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

3. Depending on the degree to which information is organised and structured, you will need to search the following non-exhaustive areas: 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. which your area is responsible for or owns.

4. You must not withhold information because you believe it will be misunderstood; instead, you should provide an explanation with the information. You must provide the information in an “intelligible form”, which includes giving an explanation of 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 effort. You may be able to agree with the requester that they will view the information on screen or inspect files on our premises. You must redact any exempt information from the released documents and explain why that information is being withheld.

5. By ensuring that the Head of Compliance has logged the request, we can ensure that we respond within the statutory timescales.

6. As the time for responding to a request does not stop during the periods when the school is closed for the holidays, we 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.

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

Guidance for communications responding to a Subject Access Request:

All correspondence must include the following information:

- a. the purposes of the processing;
- b. categories of personal data concerned;
- c. the recipients or categories of recipients to whom personal data has been or will be disclosed, in particular in third countries or international organisations, including any appropriate safeguards for transfer of data, such as Binding Corporate Rules or EC model clauses;
- d. where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period;
- e. the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- f. the right to lodge a complaint with a supervisory authority;
- g. if the data has not been collected from the data subject: the source of such data;
- h. 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.