



Subject Access Request Policy and Procedure

B – School Administration Policies & Procedures

Key author	Director of Finance & Operations
Audience	Employees; Parents
Approval body	Data Protection Committee
Approval frequency	3 years
Last approved	December 2024
Date of next review	December 2027
Published	Classlink; portal; website
Linked policies	Data Protection Policy

Contents

Document Control	1
Guidance on use	3
Data Access Request Policy	4
Introduction	4
Scope	4
Data Protection Terms	4
Background	5
General Policy	5
Subject Access Rights Procedure	6
Introduction	6
Process	6
Receipt of Subject Access Requests	7
Data Subject Identification	7
Analysis of the Request	8
Requesting Clarification (if necessary)	8
Identify and Retrieve the Data	8
Response	9

Subject Access Request Policy

Introduction

This Subject Access Request Policy (“Policy”) establishes [The British School al Khubairat](#) (“we”, “our”, “us”) commitment to complying with lawful data subject access requests.

The Senior Leadership Team is responsible for approving this Policy. Our Data Protection Committee/Board of Governors is responsible for reviewing this Policy on a regular basis. You can contact our Data Protection Committee by emailing dataprotection@britishschool.sch.ae if you have any questions or concerns. Our Assistant Head Digital of Pedagogy, Innovation & Safety is responsible for implementing this Policy.

This Policy applies to all data subjects whom we process personal data regarding including students.

This Policy applies to all staff at [The British School al Khubairat](#)

In accordance with our [Data Protection Policy](#), we commit to utilising this Policy to ensure the correct and lawful treatment of personal data and to protecting the confidentiality and integrity of personal data.

Scope

This Subject Access Request Policy applies in respect of all the Personal Data we process about our current, past and prospective students (and their parents/carers), our current and past staff members, our suppliers and any third parties with whom we communicate.

This policy sets out how we will process Personal Data. The following policies are also relevant for this purpose:-

- Privacy Policy
- Information Rights Policy
- Our Admissions Privacy Notice
Retention Schedule / Policy

Data Protection Terms

For the purposes of this policy, the following terms apply:-

Data subjects are all individuals about whom we hold Personal Data.

Personal Data means any information relating to an individual who can be identified from that information or from any other information we may hold. Personal Data can include names, identification numbers, addresses (including IP addresses), dates of birth, financial or salary details, education background, job titles and images. It can also include an opinion about an individual, their actions or their behaviour. Personal Data may be held on

paper, in a computer or any other media whether it is owned by the organisation or a personal device.

Processing means any activity which is performed on Personal Data or Special Category Data. It includes the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction of data.

Background

Under the Federal Decree-Law No. 45 of 2021 regarding personal data protection (“PDPL”) which was released on September 26th 2021, published in the official gazette November 27th 2021, and was effective on January 2nd 2022, individuals have certain rights regarding their data held by organisations. For example, individuals have the right to ask if their personal information is used or stored at the school. They may request copies of their personal information, and do so either verbally or in writing. In Europe, such requests are commonly known as subject access requests (SAR) or data subject access requests (DSAR). There is no distinction between the two terms.

There are specific requirements in the PDPL for responding to such requests and to do so without undue delay. The only grounds for refusing a subject access request is if an exemption applies, or if the request is manifestly unfounded or excessive.

General Policy

We shall comply with all lawful Data Subject Requests as required by law.

Subject Access Rights Procedure

Introduction

This Subject Access Request Procedure (“Procedure”) sets out how **The British School Al Khubairat** (“we”, “our”, “us”) will respond to any subject access requests.

The Senior Leadership Team is responsible for approving this Procedure. The **[INSERT role]** shall be responsible for implementing and maintaining this Procedure and regularly reporting relevant updates regarding the implementation of this Procedure to the **[INSERT role]**.

This Procedure applies to all data subjects whom we process personal data regarding including students as well as parents/legal guardians submitting data subject requests relating to their child’s personal data.

This Procedure applies to all staff at **The British School Al Khubairat**

In accordance with our **Data Protection Policy** and the Subject Access Rights Policy, we commit to utilising this Procedure to ensure the correct and lawful treatment of personal data and to protecting the confidentiality and integrity of personal data.

Process

There are six steps to our Subject Access Request Process

1. Receipt of Subject Access Request
2. Data Subject Identification
3. Analysis of the Request
4. Request for Clarification (If Necessary)
5. Identify and Retrieve the Data
6. Response

All Subject Access Requests will be handled in accordance with this Procedure so as to ensure that the school maintains proper documentation

1. Receipt of Subject Access Requests

Subject Access Requests can be received in a written or verbal format. Subject Access Requests (SAR’s) can be received in a written or verbal format using the following channels.

Email: Primary contact: dataprotection@britishschool.sch.ae
Subject line: **Subject Access Request - [Your Full Name]**
Include necessary details as outlined in the SAR process.

Phone: Data Protection Contact Number: +971 22040200
Inform the operator that you are requesting to submit a Subject Access Request.

Mailing Address:

British School Al Khubairat (BSAK)

Attn: Data Protection Committee

25 Um Salamah Street

P.O. Box 4001

Abu Dhabi, UAE

In-Person:

Data Subjects may submit SARs directly at the school's **main reception**. Ensure to clearly state that the request pertains to data access rights.

Requests can come directly from the individual¹ or from another person who has the authority to request (e.g. a parent). Requests do not need to include any specific language or be directed to a particular person or office at the School to be considered valid. Rather, a request is valid if it is clear that the individual is asking for access to their own personal data or that of another person if the requestor has the authority to request such personal data (e.g. a parent).

If the request is coming from a person who is requesting access to the personal data of another person (e.g. attorney requesting access to the personal data of a client), it is the third party's responsibility to provide evidence of their authority to do so.

Upon receiving the data subject request, the recipient of the request must forward the request to the **[INSERT role]** within **72** hours after receiving the request. Requests submitted through social media channels shall be forwarded to the **[INSERT role]** by the **Head of Communications**. The **[INSERT role]** will then create a record of the request within the Data Subject Access Log ("Log").

Ideally all requests should indicate:

- the name of the requestor;
- the name(s) of the relevant data subject(s) (if different);
- the date that the request was received;
- what specific information is being sought (if specified); and
- response due date (i.e. [x] days from the date of receiving the request).

Recording the date is particularly important since all requests must be satisfied within **28** days.²

¹ In the United Kingdom,, before responding to a Subject Access Request for information held about a child from the child, you should consider whether the child is mature enough to understand their rights. If the request is from a child and you are confident they can understand their rights, you should usually respond directly to the child. You may, however, allow the parent or guardian to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child. If a child is competent, they may authorise someone else, other than a parent or guardian, to make a SAR on their behalf.

² For example, in the EU organisations must comply without undue delay and at the latest within one month of receipt of the request. The time limit can be extended for a further two months if the request is complex or multiple requests have been made by the data subject. Note: there are no special timing exemptions if the access request is made during school holidays

2. Data Subject Identification

After recording the request within the Log, the [INSERT role] shall take reasonable steps to verify that the requestor is indeed who they state that they are. This will involve requesting additional information as necessary to confirm identity. The request for identification information should not be disproportionate.

If the [INSERT role] is unable to verify the identity of the requestor then the [INSERT role] shall inform the requesting individual of the reasons why, and their right to make a complaint to the [INSERT relevant data protection authority].

3. Analysis of the Request

If the [INSERT role] is able to verify the identity of the requestor (and, in the case of a request regarding access to different person's personal data, the authority of the requestor), that employee shall then conduct an analysis of the request itself seeing if any exemptions³ apply that would limit/prohibit the fulfilment of the request. For example:

- Analysing the Breadth (requests which are deemed to be manifestly unfounded or excessive or repetitive can be refused).
 - A request may be considered manifestly unfounded if the individual has no clear intention to access the information, is discernibly malicious in intent, or is using the request to harass the organisation with no real purposes other than to cause a disruption.
- Analysing the Scope: Requests can be denied if provisioning access to the requested information would affect the rights and freedoms of other data subjects (e.g. if the data is inextricably linked to the personal data of another individual).
- Identifying whether providing access would be Contrary to Other Obligations: A request can be rejected if providing the requested access would be harmful to national security, public safety, or would be likely to cause serious harm to the physical or mental health of any individual.

If the [INSERT role] identifies that an exemption applies resulting in a refusal to comply with a request, the [INSERT role] must inform the requesting individual of the reasons why, and their right to make a complaint to the UAE Data Office.

4. Requesting Clarification (if necessary)

The [INSERT role] may seek clarification from the requestor, via contacting them using available contact information if more information is needed to fulfil the request (if no exemption applies). Specifically, the [INSERT role] shall clarify the type of information or processing activities to which the request is related.

5. Identify and Retrieve the Data

Analyse the request to make sure you know what is being sought. Identify all sources and records that may hold the personal data that the individual is requesting. This may involve consulting the records of processing to determine which files may be relevant based on the type of person requesting the data (e.g. student, parent, staff member, etc.) You will

³ Exempts are unique based on the jurisdiction. The listed exemptions are merely examples, your school should work with your 9ine consultant to identify exemptions that are applicable to you.

likely also have to identify what information systems the personal data was stored within to determine if that data was shared with third parties (e.g. data processors, vendors, service providers, etc.) and then identify those third parties. Retrieve and review the identified records to confirm that they actually contain the personal data requested. Make a copy of the information for the data subject (e.g. for paper copies, photocopy the documents). If information in a document is retained in a format different from the one in which it was initially collected, then it is permissible simply to provide access in this alternative format. For instance, if a telephone call was taped, you may provide access to a log of the phone conversation. You may also be able to disclose a disc of the recording. In cases where a large number of documents are involved, you may consider inviting the requester to simply look at the documents at your premises. If acronyms, abbreviations, or codes have been used, those should be defined.

To accommodate a disability, some people may ask to receive their personal information in alternate formats, such as audio files for individuals with visual impairment. You should fulfil this request if the information already exists in the alternate format, or if conversion to that format is reasonable and necessary for an individual to exercise rights

Upon request, you should also explain how the personal information was used by your organisation. If it was shared with third parties, provide a list of them. If that is not feasible, indicate the organisations with which it may have been shared.

If the personal information in question is of a sensitive medical nature, you may consider providing access through the requester's medical practitioner, such as a physician or a psychiatrist.

If more time is necessary to respond to the request, you may request an extension from the requester in certain circumstances.⁴

6. Response

If no personal data is held on the data subject, the [INSERT role] shall inform the data subject.

If personal data is held on the data subject and no exemption exists (as identified in Step 3), the [INSERT role] shall provide the information to the requestor. The provided data must be presented in an accessible, concise and intelligible format. Where the data subject makes the request by electronic form means, the [INSERT role] shall provide the requested information by electronic means where possible, unless otherwise requested by the data subject.⁵

⁴ These circumstances vary by jurisdiction.

⁵ In addition to receiving a copy of the personal data, GDPR Article 15 also provides that data subjects have the right to obtain the following information:

- The purposes of the processing (e.g. CCTV video surveillance for security at school entrance hall).
- The categories of personal data concerned (e.g. video surveillance images)
- The recipients of the personal data (e.g. school security personnel and facilities manager).
- How long the personal data is stored or the criteria used to determine that period (e.g. 28 days from collection)
- The existence of the right to request rectification, erasure, or restriction of processing of personal data concerning the data subject or to object to such processing

When providing the information, include the name and contact information of someone in your organisation who can respond to any questions the individual may have.

Keep a copy of any documents as they were sent, subject to appropriate retention policies. Also, the response should inform individuals that they have a right to complain to the **UAE Data Office** about issues related to their request

-
- The right to lodge a complaint with [RELEVANT DATA PROTECTION AUTHORITY].
 - Information on how the personal data was collected if not collected from the data subject (e.g. data collected from a single 24-hour CCTV camera located at the school entrance hall recording video images of all people entering or leaving)
 - If applicable, the existence of automated decision-making and details of the nature and effects of such processing.
 - Where data is transferred outside the UK (or outside the EEA) the right to be informed of the appropriate safeguards.