Information Rights Policy

B – School Administration Policies & Procedures

Key author	Director of Finance & Operations
Audience	Parents
Approval body	Data Protection Management Committee / Finance & Resources Committee / BoG
Approval frequency	Annually
Last approved	November 2025
Date of next review	November 2026
Published	Parent Portal; Website; Classlink
Linked policies	Data Protection Policy, Subject Access Request Policy, Records Retention Policy, Privacy Notices. ADEK Digital Policy.

Contents

Information Rights Policy

Introduction

This Information Rights Policy ("Policy") establishes The British School Al Khubairat (BSAK)'s commitment to complying with lawful requests related to data subjects' information rights.

The Data Protection Management Team is responsible for approving this Policy. The Director of Finance & Operations shall be responsible for implementing and maintaining this Policy and regularly reporting relevant updates regarding the implementation of this Policy to the Data Protection Management Team.

This Policy applies to all staff at The British School Al Khubairat (BSAK).

In accordance with our Privacy Policies, 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 Information Rights Policy ("Policy", also known as "Data Subject Rights Policy") applies in respect of all the Personal Data we process about all data subjects. This includes current, past and prospective students (and their parents/legal guardians), our current and past staff members, our suppliers and commercial customers, contractors and any third parties with whom we communicate.

This policy sets out how we will respond to information rights requests. The following policies are also relevant for this purpose:-

- Privacy Policy
- Subject Access Request Policy
- Our General Privacy Notice
- Admissions Privacy Notice
- Employee 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.

Information Rights (also referred to as data subject rights or individuals' rights) refer to the legal rights provided to data subjects concerning their relationship to their personal data held by third parties, which in this case means our School.

Information Rights Request means any request from a data subject to invoke an information right. The request does not have to be in a particular form and does not need to include particular terms/words in order to be valid (e.g. a person doesn't state that they would like for their data to be erased in order for the right to erasure to be invoked) – all it has to do is supply sufficient information so as to convey what information right the data subject is interested in invoking (e.g. if the data subject is interested in receiving a copy of the personal data within the school's control).

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.

Process/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.

Requestor means the data subject who submitted the request to invoke one or more information rights available to them.

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 pertaining to their personal data held by organisations. These rights are not absolute and are subject to certain restrictions. The rights are:

- the right to be informed: individuals have the right to be provided with clear and concise information about how we process their personal data. We satisfy this through our Privacy Notices/Policies.
- the right of access: individuals have the right to request and obtain detailed information about the types of personal data being processed, how it is being protected as well as other supplementary information to help them understand how and why we are using their personal data.
- the right to rectification: individuals have the right to have inaccurate personal data corrected. In certain circumstances, individuals may also request that we supplement the existing personal data we control on the individual if it is deemed to be incomplete.
- the right to erasure: individuals have the right to have their personal data erased.
- the right to restrict processing: individuals can limit the way that we use their data.

- the right to data portability: individuals have the right to receive their personal data they have provided to us in a structured, commonly used and machine-readable format. Individuals also have the right to request that we transmit this personal data directly to another controller (e.g. another school).
- the right to object to processing: individuals have the right to stop or prevent us from processing their personal data.
- the right to avoid automated decision making (including profiling): individuals have the right to object to their personal data being used to make decisions by automated means without any human involvement.

These rights are often referred to collectively as either information rights or data subject rights. There is no functional difference between the terms.

There are specific requirements under the Federal Decree-Law No. 45 of 2021 regarding personal data protection ("PDPL") for responding to such requests. There are only certain situations in which such requests may be refused and there are time limits in which such requests must be fulfilled. Moreover, in our country, we can not charge fees for fulfilling individual rights. Furthermore, as a data subject you have the right to complain to the UAE Data Office if you believe a violation of the regulation has occurred.

General Policy

We shall handle all lawful requests we receive relating to data subjects' information rights in a legally compliant manner.

Subject Access Request Procedure

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 writing or verbally. Information Rights Requests can be received in a written or verbal format by contacting dataprotection@britishschool.sch.ae or via Tel on: +971 22040200. Requests can come directly from the individual or from another person who

has the legal authorisation to request on behalf of the data subject (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 personal data (or that of another person if the requestor has the authority to request such personal data). If it appears that the data subject is invoking a different information right (e.g. right to erasure) or if the data subject is simultaneously invoking multiple information rights then the Procedure for All Other Rights should be followed for any requests other than subject access requests

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.

If there is any ambiguity regarding whether the data subject is invoking a right to request access, the staff member who receives the request should clarify with the data subject if they are indeed requesting access. We are obligated to assist data subjects who submit information rights requests if they request assistance.

Upon receiving the data subject request, the recipient of the request must forward the request to the Data Protection Management Team within 72 hours after receiving the request. Requests submitted through social media channels shall be forwarded to the Data Protection Management Team Officer or Equivalent by the Communications & Marketing Department.

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; and
- what specific information is being sought (if specified);

The Data Protection Management Team will then create a record of the request within the Data Subject Rights Request Log ("Log") and send via email, a letter acknowledging that the request has been received and is being processed.

Recording the date is particularly important since all requests must be satisfied within a reasonable period and without undue delay.

2. Data Subject Identification

After recording the request within the Log, the Data Protection Management Team shall determine if there are any reasonable doubts concerning the identity of the person submitting the request.

- If not, the Data Protection Management Team shall send an acknowledgement to the requester. Then proceed to Step 3 of this Procedure.
- If so, 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 shall not be disproportionate, a government-issued

photo identification card or a school-issued identification card will suffice. The information will be securely stored and deleted once it is no longer required.

- If the identity can be confirmed, the Data Protection Management Team shall send an acknowledgement to the requester. Then proceed to Step 3 of this Procedure.
- If not, Data Protection Management Team shall send a letter or email (depending on the contact information available) to the requestor specifying the need for further proof of identity in order to proceed with the request,

If the person submitting the request is different from the data subject at issue (or the person's parent in the case of an individual under the age of 18), the requestor will also need to supply evidence that they have the authorisation from the individual to submit the request on the individual's behalf. For parents invoking a right on behalf of their child, for example, We will need to be satisfied that the person invoking the right is indeed the parent/legal guardian of the child in question.

If the Data Protection Management Team is unable to verify the identity of the requestor then the Data Protection Management Team shall inform the requesting individual of the reasons why, and their right to make a complaint to the UAE Data Office.

3. Analysis of the Request

If the Data Protection Management Team 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 exemptions apply that would limit/prohibit the fulfilment of the request. For example:

- Analysing the Breadth (generally, requests which are deemed to be unrelated to information that can be accessed under this right or to be repetitive can be refused).
  -
  - We can ask the requesting data subject to specify what personal data or processing activities they would like to access.
- Analysing the Scope: Requests can be denied if provisioning access to the requested information would affect the privacy and confidentiality of other data subjects (e.g. if the data is inextricably linked to the personal data of another individual).
- Identifying whether Providing Access would conflict with judicial procedures or investigation
- Analysing the Impact: Requests can be denied if they will adversely affect the school's efforts to protect information security.

If the Data Protection Management Team identifies that an exemption applies resulting in a refusal to comply with a request, the Data Protection Management Team 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 Data Protection Management Team may seek clarification from the requestor, via contacting them using available contact information if more information is needed to fulfill the request (if no exemption applies). Specifically, the Data Protection Management Team 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 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 the requested personal data (including, as necessary, from any data processors who hold any of the personal data) 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 fulfill 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.

6. Response

If no personal data is held on the data subject, the Data Protection Management Team shall inform the data subject.

If personal data is held on the data subject and no exemption exists (as identified in Step 3), the Data Protection Management Team shall provide the information to the requestor. The provided data must be presented in an accessible, concise and intelligible format. If the request for information is relating to a child or has been made by a child, the following considerations need to be made:

- Where possible the child's level of maturity and their ability to understand and interpret the information they receive.
- Any court orders relating to parental access or responsibility that may apply.
- Any duty of confidence owed to the child.
- Any consequence of allowing those with parental responsibility access to the child's information, particularly if there have been allegations or investigations in the past.

Where the data subject makes the request by electronic form means, theData Protection Management Team shall provide the requested information by electronic means where possible, unless otherwise requested by the data subject.

Procedure for All Other Rights

Process

There are six steps to our All Other Rights Procedure
1. Receipt of Data Subject Request
2. Analysis of the Request
3. Identification/Authorisation Verification
4. Request for Clarification (If Necessary)
5. Fulfill the Request
6. Response

1. Forwarding Information Rights Request to Data Protection Team

Information Rights Requests can be received in a written or verbal format by contacting dataprotection@britishschool.sch.ae or via Tel on: +971 22040200. Requests can come directly from the individual 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 to be considered valid.

All subject access requests we receive will be handled in accordance with the Subject Access Request Procedure. All requests relating to the following rights are handled in accordance with this procedure:

- The Right to Information;
- The Right of Access;
- The Right to Rectification;
- The Right to Erasure;
- The Right to Restriction of Processing;
- The Right to Data Portability;
- The Right to Object; and
- The Right to Avoid Automated Decision-Making.

Any request that includes a subject access request and an invocation of a different right (e.g. right to restrict processing) will be separated into their component requests and handled in accordance with the appropriate procedure (e.g. the subject access request component would be handled in accordance with the Subject Access Request Procedure and the request to restrict processing would be handled in accordance with this Procedure).

The request must then be emailed to the Data Protection Management Team at dataprotection@britishschool.sch.ae

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; and
- what specific information is being sought (if specified)/what right is being invoked (if discernible)

2. Identification of the Right(s) Being Invoked

After receiving a request:

- If there is any ambiguity regarding whether the data subject is invoking an information right, the staff member who receives the request should forward the request to dataprotection@britishschool.sch.ae. That person will follow up with the requestor and to clearly understand what is being requested. For example, if a particular processing activity's lawful basis is consent and a data subject who previously provided consent subsequently withdraws consent, that request could be intended by the data subject as a request for erasure even if the data subject doesn't include those terms it will be imperative to clarify whether that is the data subject's expectation in that situation. We are obligated to assist data subjects submit information rights requests if they request assistance; or
- If it is clear that the data subject is invoking an information right other than a subject access request, the individual who received the request will forward the request (e.g. the letter, or the email, or if the request was an in-person/voicemail request then the staff member who received the request shall type an email explaining the request) to the Data Protection Management Team within 72 hours after receiving the request. Requests submitted through social media channels shall be forwarded to the Data Protection Management Team by the Communications & Marketing Department.

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 a reasonable amount of time and without undue delay.

The Data Protection Management Team will then create a record of the request within the Information Rights Request Log ("Log") and send via email a letter acknowledging that the request has been received and is being processed.

3. Identification of the requestor and ensuring proper authorisation to fulfill request

After recording the request within the Log, the Data Protection Management Team 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 information will be securely stored and deleted once it is no longer required. The request for identification information shall not be disproportionate, a government issued photo identification card or a school issued identification card will suffice.

If the person submitting the request is different from the data subject at issue (or the person's parent in the case of an individual under the age of 18), the requestor will also need to supply evidence that they have the authorisation from the individual to submit the request on the individual's behalf. This often will take the form of a letter establishing a client-attorney relationship between the individual and the person submitting the request or a power-of-attorney naming both the data subject at issue and the person submitting the request.

If the Data Protection Management Team is unable to verify the identity of the requestor (or that person's authority to issue the request, if the request is coming from someone other than the data subject or the data subject's parent/legal guardian if the data subject is under the age of 18), then the Data Protection Management Team shall must inform the requesting individual of the reasons why, and their right to make a complaint to UAE Data Office

4. Checking for Exemptions

If the Data Protection Management Team 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 to submit the request), that employee shall first conduct an analysis of the request itself to determine whether any legal exceptions exist which would prohibit the fulfillment of the request.

Generally speaking, controllers may charge a reasonable fee (based on administrative costs) or refuse to act if requests are manifestly unfounded or excessive particularly due to repetition of the same request

Right-specific exemptions also exist which would allow the school to refuse/limit fulfillment of a information rights request, including:

- The Right to Erasure

- Any request that is unrelated to one of the following:
  - the personal data is no longer necessary for the purpose which we originally collected or processed it for;
  - we are relying on consent as your lawful basis for holding the data, and the individual withdraws their consent;
  - we have processed the personal data unlawfully (ie in breach of the lawfulness requirement of the 1st principle);
  - Where there is no legitimate reason to continue processing
- Moreover, the right to erasure does not apply if processing is necessary for one of the following reasons:
  - If erasure would affect investigation procedures, claims for rights and legal proceedings or defense by the controller; or
  - If erasure would conflict with other legislation to which the school must comply.

- The Right to Restriction of Processing
  - If the request does not relate situations where:
    - the data subject objects to its accuracy, in which case processing shall be restricted to a specific period allowing the school to verify accuracy of the data;
    - the data subject objects to processing of their personal data in violation of agreed purposes;
    - processing is in violation of the Federal Law.
  - Moreover, the right to restriction does not apply if processing is:
    - limited to only the storing personal data;
    - necessary to initiate or defend against any actions to claim rights or legal proceedings, or related to judicial procedures;
    - necessary to protect third party rights;
    - necessary to protect the public interest.

- The Right to Data Portability
  - If the personal data was not processed:
    - On the basis of consent or for the performance of a contract; and
    - by automated means (ie excluding paper files).

- The Right to Object
  - If the personal data processing is not:
    - For direct marketing purposes, including profiling related to direct marketing;
    - to conduct statistical surveys, unless the processing is necessary to achieve the public interest;
    - in violation of data processing principles.

- The Right to Object to Automated Decision-Making.
  - Where automated processing does not have legal consequences or seriously affect the Data Subject, including Profiling.
- Moreover, the data subject may not object to the decision issued if

- the automated processing is included in the terms of the contract entered into between the Data Subject and school.
- the automated processing is necessary according to other legislation in force in the State.
- the data subject has given his/her prior consent on the Automated Processing
-

5. Fulfilling the Request

If no exemptions apply, then the Data Protection Management Team shall fulfill the request to the best of their ability. Generally speaking this means, for requests concerning:

- The Right to be Informed
  - Supplying the requestor with the applicable Privacy Notices/Privacy Policies. For example, if a website visitor contacts the school to ask about what data we collect from website visitors, we would supply a copy of our Privacy Notice/Privacy Policy Governing Website Visitors.

- The Right to Rectification
  - The Data Protection Management Team shall investigate the personal data in question in light of the request to determine whether the personal data is accurate or if there is any need to rectify the data. The end goal is that all of the personal data we control needs to be as accurate and complete as possible and, towards that end, if some of the personal data or all of the personal data needs to be rectified in light of the request in order to make the personal data we control more accurate and complete then the Data Protection Management Team shall take whatever steps necessary to rectify any inaccuracies or incomplete entries. Rectification decisions are not a dichotomous decision (in terms of rejecting all of the changes proposed by the data subject or none of them), rather the Data Protection Management Team shall investigate every identified personal data entry in question on a one-by-one basis to determine whether any changes need to be made taking into account the arguments and evidence provided by the data subject.
  - Evidence will be obtained of the accurate data and once validated, the data in question will be rectified.
  - The more important it is that the personal data is accurate, the greater the effort you should put into checking its accuracy and, if necessary, taking steps to rectify it. Importance in this context relates not only to the sensitivity of the personal data (e.g. whether the personal data includes any special category data) but also about the degree to which the processing activity itself which uses the personal data would be impeded by incorrect or incomplete personal data.
  - If there is a question about the accuracy or completeness of personal data in the form of an opinion, as long as the Record of Processing identifies that the personal data is an opinion and, where appropriate, whose opinion it is, it is likely difficult to determine if it is inaccurate and needs to be rectified.

- If a decision is made to rectify any personal data that has been shared with any third party (e.g. data processors), the Data Protection Management Team shall contact each recipient and inform them of the rectification or completion of the personal data unless this proves impossible or involves disproportionate effort. If asked to, you must also inform the individual about these recipients.

- The Right to Erasure
  - If the Data Protection Management Team determines in Step 4 (above) that the request is based on an approved basis, then the Data Protection Management Team shall identify all relevant personal data relating to the request and securely dispose of it in accordance with our Records Management Policy. This is particularly true for any erasure request submitted by (or on behalf of by a parent) a child or anyone who provided their personal information at a time when they were a child. This is because, despite our best efforts to inform children of the consequences of processing their personal data, children may nevertheless not have been fully aware of the risks involved in the processing at the time of consent.
  - If the Data Protection Management Team determines that erasure is necessary in light of the request, and if we have disclosed the underlying personal data to others (e.g. data processors), the Data Protection Management Team shall contact each other party and inform them of the erasure, unless this proves impossible or involves disproportionate effort.
  - If a valid erasure request is received and no exemption applies then the Data Protection Management Team shall work with all relevant school staff and other necessary individuals to ensure the personal data's erasure from backup systems as well as live systems.
  - The data in question will be deleted from all locations where it is held, including physical/digital archives, retrievable backups etc.
  - Where we had previously transferred the personal data in question to other parties (e.g. data processors), the Data Protection Management Team shall communicate the erasure request to those parties.

- The Right to Restriction of Processing
  - After it is determined that no exemptions apply, the Data Protection Management Team shall verify that the requestor supplied a particular reason for the request. There is no "right" or "wrong" reason per se, the important thing is that a reason is provided, For example, this may be because the data subject has concerns with the content of the personal data process about them.
  - The data in question will be kept but not processed in ways that would misalign with the expectations of the requester.
  - The Data Protection Management Team shall consult, as necessary, with any staff member or external consultant to identify the best way(s) of restricting access. For example, some methods include:
    - temporarily moving the data to another processing system;
    - making the data unavailable to users; or
    - temporarily removing published data from a website.

- The Data Protection Management Team will then have to determine the length of time that the restriction will need to be in place. Most often, we won't be required to restrict an individual's personal data indefinitely, but will need to have the restriction in place for a certain period of time. The length of time will depend on a number of factors including the reason for the request, the sensitivity of the personal data, and whether further restriction serves its identified purpose (i.e. if the request for a restriction was based on a request for rectification and all identified inaccuracies in the individual's personal data have been rectified then the processing restriction may not need to be restricted any further than the date that the incorrect personal data was rectified).
    - If/once it is determined that it is appropriate to lift the restriction on processing the personal data, the Data Protection Management Team must inform the individual before lifting the restriction.
- Even if processing certain personal data is restricted in light of this procedure, it can still be stored (e.g. in its existing databases) so long as it is not processed otherwise unless:
    - We have obtained the individual's consent for processing;
    - Processing is for the establishment, exercise or defence of legal claims;
    - Processing is for the protection of the rights of another person (natural or legal); or
    - Processing is for reasons of important public interest.
- If personal data is restricted in accordance with this procedure and if we have disclosed the personal data in question to other parties (e.g. data processors), the Data Protection Management Team must contact each recipient and inform them of the restriction of the personal data - unless this proves impossible or involves disproportionate effort. If asked by the requestor, the Data Protection Management Team must also inform the data subject that other parties had previously been transferred the personal data

- The Right to Data Portability
    - Information is only within the scope of the right to data portability if it is personal data of the individual that they have provided to us.
        - This includes not only information consciously supplied by the data subject (e.g. in a form) as well as personal data resulting from observation of an individual's activities (e.g. history of website usage)
        - It does not include any additional personal data we create based on the personal data an individual has provided to you (e.g. a student profile).
    - The right to data portability only applies to personal data (i.e. information about an identifiable individual). This means that it does not apply to genuinely anonymous data (since it doesn't relate to an identifiable person).
    - If the personal data that was requested includes other data subjects' personal data, the Data Protection Management Team shall consider whether transmitting that data would adversely affect the rights and freedoms of those third parties. Generally speaking, providing such personal data of other data subjects to the requestor should not be a problem if the requestor provided this data to us as a part of their own personal data they submitted to us (e.g. if a student submitted the names of his parents).

- If the requested personal data was initially provided by multiple data subjects, the Data Protection Management Team will need to verify that all parties who submitted the personal data agree to the portability request.
- If the Data Protection Management Team determines that the request for data portability meets all criteria outlined above:
  - the requestor is entitled to securely:
    - receive a copy of their personal data; and/or
    - have their personal data transmitted from one controller to another controller.
      - The Data Protection Management Team shall consider the technical feasibility of a transmission on a request by request basis.
  - Data Protection Management Team shall facilitate this either by:
    - directly transmitting the requested data to the individual; or
    - providing access to an automated tool that allows the individual to extract the requested data themselves.
      - Such access shall be strictly limited to enable the requestor to perform the sole function of extracting their personal data.

  - We shall provide this personal data in a format that is:
    - Structured;
      - software must be able to extract specific elements of the data (e.g. a spreadsheet where the data is organised into rows and columns)
    - commonly used (e.g. CSV, XML and JSON formats); and
    - Machine-readable.
      - E.g. Transmitting information via an application programming interface ("API").

- The Right to Object
  - The Data Protection Management Team shall identify the scope of the request. An objection request may relate to all of the personal data we hold about the requestor, or only a subset thereof. It may also only relate to a particular purpose for which we are processing the personal data.
  - For any requests pertaining to our direct marketing efforts, there are no exemptions or grounds for us to refuse such requests (or at least the aspect of a more broad request that includes objecting to our direct marketing efforts). Therefore, if we receive an objection to processing for direct marketing, the Data Protection Management Team must ensure that any existing processing of the requestor's personal data for that purpose stops.
    - In such situations, we shall retain the minimum amount of information about the requestor to ensure that their preference not to receive direct marketing is respected in future.
  - The requestor must provide (either in their initial request or in response to a follow-up communication from the Data Protection Management Team specific reasons why they are objecting to the processing of their data.

- Where we have received an objection to the processing of personal data and we have no grounds to refuse, we will stop or not begin processing the data. The Data Protection Management Team will need to determine, on a case-by-case basis, how best to comply. The data in question will no longer be processed for the specified purpose(s).
    - This may mean that we need to erase personal data, as the definition of processing under 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, which includes storing data.
    - Yet, this will not always be the most appropriate action to take. For example, erasure may not be appropriate if we process the data for other purposes as we need to retain the data for those purposes.

- The Right to Avoid Automated Decision-Making.
    - Where we have received an objection to the processing of personal data and we have no grounds to refuse, we will stop or not begin processing the data. The Data Protection Management Team will need to determine, on a case-by-case basis, how best to comply.
    - The process will not be completed via an automated system and will require the most relevant school member to act in replacement of the system. A response will be provided to the data subject to inform them of the output determined.

6. Response

All responses shall be built off of the template subsequent response letter.
Regardless as to whether the Data Protection Management Team decides to fully, partially, or not comply with an information rights request, a response must be provided to the requestor.

- All Responses must
    - Be written
        - in a clear, concise, transparent, intelligible, and easily accessible form;
        - Clearly articulate what we did (or did not do).
            - For example, if we did not comply with a rectification request, we shall let the requestor know that after investigating the issue we were satisfied that the personal data in question is accurate, and as such we will not be amending the data.
            - This is particularly important for responses regarding requests for erasure that are being fulfilled. For example, when referencing any personal data that was processed in backup systems, It may be that the erasure request can be instantly fulfilled in respect of live systems, but that the data will remain within the backup environment for a certain period of time until it is overwritten.
        - Using plain and clear language:
            - particularly when addressed to children or other vulnerable groups

- Be provided without undue delay and within a reasonable time after the initial request, Provide the following information
  - The name and contact details of our organisation.
  - The name and contact details of our representative (if applicable).
  - The contact details of our data protection officer (if applicable).
  - The rights available to individuals in respect of the processing.
  - The right to lodge a complaint with a supervisory authority.
- Where requests are made electronically:
- Any personal data we transfer to the requestor (e.g. in light of a request for access or a request for data portability) must be provided electronically, unless otherwise requested by the individual.
  - Regardless of how we transfer any personal data, we are responsible for the personal data until it is received by the requestor (or the designated third party, in the case of certain data portability requests). As such, all transmissions of personal data must be done securely and in accordance with our Data Protection Policy.
- Be free of charge to the requestor.
- If the request for information is relating to a child or has been made by a child, the following considerations need to be made:
  - Where possible the child's level of maturity and their ability to understand and interpret the information they receive.
  - Any court orders relating to parental access or responsibility that may apply.
  - Any duty of confidence owed to the child.
  - Any consequence of allowing those with parental responsibility access to the child's information, particularly if there have been allegations or investigations in the past.
- Additionally, if an exemption applies or if we otherwise decide not to comply with a requestor's information rights request we shall, within a reasonable time of receiving the request, inform the individual about:
- the reason(s) for not taking action;and
- their remedies, in particular the right to:
- Lodge a Complaint with the UAE Data Office.

Copies of all information that is provided to a data subject will need to be kept by the Data Management Team as evidence. This may be required by the regulator in the event of an audit.