Data Protection Policy

B – School Administration Policies & Procedures

Key author	Director of Finance & Operations
Audience	Employees; Parents
Approval body	Finance & Resources Committee / BoG
Approval frequency	3 years
Last approved	October 2024
Date of next review	October 2027
Published	Classlink; portal; website
Linked policies	Our General Privacy Notice, Retention Schedule / Policy, CCTV Policy, Subject Access Rights Policy.

Table of Contents

Introduction

At The British School Al Khubairat, we acknowledge the importance of data protection and recognise that individuals have rights in respect of the Personal Data we handle.

During the course of our business activities, we will collect, store and process personal data. We will endeavour to treat this data in accordance with legal safeguards and in a manner consistent with the high standards individuals have come to expect from our organisation.

All our staff members are required to comply with this Data Protection Policy when processing Personal Data as part of their role. Failure to comply with this policy may lead to disciplinary action.

The Data Protection Management and Reporting Team is responsible for ensuring compliance with this policy in their respective areas of responsibility.

This policy is overseen by The Director of Finance & Operations.

Scope

This Data Protection 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, our contractors, our external providers (lettings) and any third parties we communicate with.

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

- Data Incident and Breach Policy Procedure
- Our General Privacy Notice
- Retention Schedule / Policy
- CCTV Policy
- Roles and Responsibilities Policy

Data Protection Terms

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

Data Controller means the organisation which determines the purposes for processing Personal Data and the manner in which that processing will be carried out. In most cases, the School will be the Data Controller of the Personal Data it collects and uses as part of its business activities.

Data Processor means the organisation or person that processes Personal Data on our behalf and in accordance with our instructions, such as suppliers and contractors. Our staff members are not Data Processors.

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.

Special Categories of Personal Data are more sensitive, and include information revealing an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs.. It will also include data concerning health (physical and/or mental health) and data concerning genetic and biometric information where that data is used to uniquely identify a person. We will also treat data relating to criminal convictions or related proceedings in the same way as special categories of data.

Data Protection Principles

The British School Al Khubairat is responsible for and must be able to demonstrate that Personal Data is being processed in accordance with 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.

Principle One (1) - Lawfulness, Fairness & Transparency

Personal Data must be processed Lawfully, fairly and in a transparent manner.

In order to comply with this principle, we will ensure that we only process Personal Data where we are lawfully permitted to do so. We will be open and honest with individuals about the data we collect, why we use it, and which lawful basis justifies that use. We will do this via privacy notices, whether or not we collect information directly from the individuals concerned.

In addition, for each processing activity that we undertake, we will consider how that processing affects the individuals concerned.

In order to process data lawfully, we will ensure that at least one of the following lawful basis applies:

- The Data Subject has provided consent. This consent will be a freely given, specific, informed and clear indication of the individual's wishes.
- The processing is necessary for the performance of a contract with the Data Subjects such as the provision of education for a student under the parental contract).
- The processing is necessary for us to comply with a legal obligation (not a contractual obligation).
- Processing the data is necessary to protect an individual's vital interests (life or death), such as the management of a medical emergency.
- Processing is necessary to carry out a task in the public interest or where there is a clear basis in law.

- The processing is necessary for our legitimate interests, or those of a third party, so long as those interests are not overridden by the interests, rights or freedoms of the Data Subject.

Principle Two (2) - Purpose Limitation

Personal Data should be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.

In order to comply with this principle we will only process Personal Data for the specific lawful purposes set out in our Record of Processing Activity and Privacy Notices, unless we are specifically permitted to process the data by law.

Principle Three (3) - Data minimisation

Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

In order to comply with this principle, the data we collect will be sufficient to fulfil the purpose of collection (adequate), there will be a rational link between that data and the purpose (relevant) and we will only collect the Personal Data we need to fulfil the specific purpose we have collected the data for.

Principle Four (4) - Accuracy

Personal Data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay.

In order to comply with this principle, we will ensure that all Personal Data is kept up to date and is accurate. We have appropriate processes in place to check the accuracy of the data we collect and the sources of data are always recorded. We will also comply with an individual's right to rectification (see below) and we will carefully consider any challenges to the accuracy of the Personal Data.

Principle Five (5) - Storage limitation

Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed.

In order to comply with this principle, we will only keep Personal Data for as long as we need it and we will take all reasonable steps to destroy or erase all data which is no longer required. Personal Data will be kept in accordance with our Retention Policy to ensure that data is not kept any longer than necessary and we will ensure that individuals understand the duration for which their Personal Data will be held.

Principle Six (6) - Integrity and confidentiality

Personal Data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

In order to comply with this principle, we will ensure that we have appropriate organisational and technical measures in place to safeguard the security of the Personal Data we process. This includes ensuring the confidentiality, integrity and availability of the systems and services used to process the Personal Data.

Data Security

We will ensure that we have appropriate security measures in place to protect Personal Data against unlawful or unauthorised processing, and accidental loss or destruction.

In accordance with Principle 6 (Integrity and Confidentiality, above):

- We will ensure the confidentiality of Personal Data by protecting it against unintentional, unlawful or unauthorised access, disclosure or theft.
- We will ensure the integrity of Personal Data by maintaining its accuracy and protecting it against accidental or unlawful alteration.
- We will ensure the availability of Personal Data by regularly testing, assessing and evaluating the effectiveness of our technical and organisational measures to ensure our systems and services can be restored and accessed in a timely manner in the event of a physical or technical incident.

Our security measures include:

- Keeping Personal Data in paper records or on removable devices in lockable rooms, desks or cupboards and disposing of these records securely when required.
- Keeping digital Personal Data in line with our agreed policies.
- Ensuring staff members only share Personal Data they use in the course of their work with authorised personnel.
- Maintaining up to date firewalls and other IT security measures, with regular audits of our IT systems.
- Training staff on the importance of data protection and safe handling of personal data.
- Regularly auditing our governance and information management processes.

Notifying Data Subjects

Where we collect Personal Data directly from individuals or via a third party source, we will inform those individuals about the use of their data through our Privacy Notices, which will include the following details:

- The name and address of our school, as the Data Controller.
- The name and contact details of our Data Protection Officer or Data Protection Lead.
- The categories of Personal Data we are processing.
- The purpose or purposes we intend to use the Personal Data for.
- The legal basis for processing that Personal Data (and, where Special Categories of Personal Data are being processed, the additional processing condition allowing this).
- The recipients of any Personal Data we share or disclose.
- Details of any transfers to other countries and what safeguards are in place.
- The length of time we will retain the Personal Data for.
- The rights Data Subjects have to access their data, or limit its use or disclosure.
- The right of Data Subjects to complain to the Regulatory Authority about our use of their Personal Data.
- The source of the Personal Data (where we receive it from a third party).
- The existence of any automated decision making (including profiling).

Data Subject Rights

We recognise that Data Subjects have a number of rights regarding our use of their Personal Data, some of which are subject to conditions. All requests will be dealt with by our Data Protection Officer or our Data Protection Lead in accordance with our Information Rights Policy.

Right of access (commonly referred to as a subject access request)

This gives individuals the right to ask us about the Personal Data we use about them. This can include what we use it for, who we share it with, how long we store it and where we have obtained it from. Individuals can also ask for a copy of their personal data.

Right to rectification

This gives individuals the right to ask for inaccurate Personal Data to be corrected or for incomplete Personal Data to be completed.

Right to erasure ('right to be forgotten')

This gives individuals the right to ask for their Personal Data to be erased but the obligation for us to erase Personal Data only applies in certain circumstances.

Right to object

This gives individuals the right to ask us not to use their Personal Data. This will include the use of their data for direct marketing, or where automated decisions have been made about them .

Rights in relation to automated individual decision-making, including profiling

This gives individuals the right to object to decisions being made about them solely by automated means (without any human involvement) and to profiling (where automated processing is used to evaluate certain things about the individual).

If we are unable to comply with a request then we will clearly inform Data Subjects about the reasons why.

Sharing and Transferring Personal Data

We will only transfer Personal Data to a Data Processor where they have provided us with sufficient guarantees that they will protect the data in compliance with data protection legislation and in line with our expectations. We will also ensure that these requirements are governed by contract or other legally binding agreement.

The School will provide information to each pupil/parent (which can include relevant personal data of the respective parent and/or child) as necessary to facilitate school operations.

We will also enter into Data Sharing Agreements with other Data Controllers, where this is considered appropriate.

Data Retention and Disposal

We do not encourage the retention of any Personal Data for any longer than necessary, in accordance with Principle 5 (Storage Limitation, above). We will ensure that all Personal and Special Category Data is disposed of in a way that protects the privacy of Data Subjects.

We will retain a Retention Schedule that details the specific types of information we handle and the appropriate periods for retention.

Dealing with Data Protection Incidents

We will manage data protection incidents in accordance with the process set out in our Incident Management Policy. As part of this process, we require all our staff members to follow specific guidelines on reporting data incidents, including completing a data incident form which we will investigate and log.

Data Protection Impact Assessments

We will carry out a Data Protection Impact Assessment when the processing of Personal Data is likely to result in a high risk to the rights and freedoms of individuals. This process is designed to identify the nature of the risks so that mitigating actions can be taken to reduce or eliminate these risks.

We will have a process in place for our staff members to follow which includes guidance about when a Data Protection Impact Assessment is required.

Use of CCTV

We use CCTV in accordance with our CCTV Policy to ensure any images we collect and use are handled appropriately.