Dubai English Speaking School & College

DESSC DATA PROTECTION Policy

2023 - 24

Author:	Malachy McGrogan	Review Date:	October 2023
Approved by:	Chris Vizzard	Next Review:	September 2024

CONTENTS		PAGE NO.
1	Rationale	2
2	Aims	2
3	Responsibilities 3.1 Staff 3.2 Parents	3
4	Implementation	3
5	Evaluation	4
6	Appendices	

DUBAI ENGLISH SPEAKING SCHOOL & COLLEGE
DATA PROTECTION POLICY

1. RATIONALE

At Dubai English Speaking School and College, 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 Senior Leadership Team is responsible for ensuring compliance with this policy in their respective areas of responsibility.

2. AIMS

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with UAE Law (e.g. UAE Penal Code, Article 379) and the principles outlined in the UK Data Protection Act 1998 and the EU General Data Protection Regulation (GDPR) 2018.

> Article 379 of the UAE Penal Code provides that it is a criminal offence for an individual to use a third party's information without consent for his own or another's advantage where that information was gained as a result of the individual exercising his profession, craft or art.

It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

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 and any third parties we communicate with.

This policy sets out how we will process Personal Data.

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 or trade union membership. It will also include data concerning health (physical and/or mental health), and 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.

3. RESPONSIBILITIES

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held.

Dubai English Speaking School and College is responsible for and must be able to demonstrate that Personal Data is being processed in accordance with the principles of the UAE DPL. This is known as the duty of accountability (see below).

The principles of data protection are [NOTE: Based on GDPR principles until such time as the UAE Framework is released]:-

Principle One - Lawfulness, Fairness & Transparency
Personal Data must be processed Lawfully, fairly and in a transparent manner.

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

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

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 - 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.

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 - 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.

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.

Principle Six - 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.

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 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 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 as they occur, following the steps detailed below. As part of this process, we will 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 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.

3.1 DESSC STAFF

The school is committed to maintaining the above principles at all times. Therefore, the school will:

- Inform individuals why the information is being collected when it is collected;
- Inform individuals when their information is shared, and why and with whom it was shared;
- Check the quality and the accuracy of the information it holds;
- Ensure that information is not retained for longer than is necessary;
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely;
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded;
- Share information with others only when it is legally appropriate to do so;
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests;
- Ensure our staff are aw are of and understand our policies and procedures.

Complaints will be dealt with in accordance with each school's Complaints Policy.

3.2 DESSC PARENTS

It is the responsibility of parents to advise the school of changes to their data. This is inclusive of any data held, such as contact information.

4. IMPLEMENTATION

Data protection breaches could be caused by a number of factors. A number of examples are shown below:

- Loss or theft of pupil, staff or governing body data and/ or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment Failure
- Poor data destruction procedures
- Human Error
- Cyber-attack
- Hacking

In the event that the School identifies or is notified of a personal data breach, the following steps should followed:

- The person who discovers/receives a report of a breach must inform the Head Teacher and/or the school's Director of Technology or, in their absence, the Senior Deputy Head Teacher. If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.
- The Head Teacher or Director of Technology (or nominated representative) must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff such as the network Operation Manager.
- It is the school's responsibility to take the appropriate action and conduct any investigation.

- The Head Teacher (or nominated representative) must consider whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future. In such instances, advice from the School's legal support should be obtained.

- The Head Teacher or Director of Technology (or nominated representative) must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

    - Attempting to recover lost data or equipment.

    - Consideration should be given to a global email to all school staff. If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer's name and contact details if possible and confirm that they will ring the individual, making the enquiry, back. Whatever the outcome of the call, it should be reported immediately to the Head Teacher (or nominated representative).

    - The use of back-ups to restore lost/damaged/stolen data.

    - If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.

    - If the data breach includes any entry codes or IT system passwords, then these must be changed immediately and the relevant agencies and members of staff informed

5. EVALUATION

This Policy will be reviewed annually.

If you have any enquires in relation to this policy, please contact *mmcgrogan@dessc.sch.ae* who will also act as the contact point for any subject access requests.

6. APPENDICES

None