مدرسة الدوحة البريطانية
DOHA BRITISH SCHOOL

Data Protection Policy

Last Review: September 2021

Next Review: June 2022

Reviewer: Policy Committee

HORSES ORYXES CAMELS FALCONS SCORPIONS

1. Purpose

Doha British School recognises the importance of storing and monitoring access of the personal data that is held on students, either on paper or in electronic form. This policy outlines specifically the data that is held on students, how it is processed and the other parties that this data can or is transmitted to. The policy is drawn up in compliance with the Law No. 13/2016 concerning Privacy and Protection of Personal Data.

2. Scope

This policy applies to all staff and organisations that work with Doha British School.

3. Definitions

DBS – Doha British school
SLT – Senior Leadership Team

4. Policy statement

Doha British School Senior Leadership Teams (SLT) has overall responsibility for ensuring that records are maintained, including security and access arrangements, in accordance with Education Regulations and all other statutory provisions.

The Principals will comply fully with the requirements and principles of the Law No. 13/2016 concerning Privacy and Protection of Personal Data. The Principal is responsible for ensuring that all staff involved with the collection, processing and disclosure of personal data are aware of their duties and responsibilities within these guidelines.

4.1. Enquiries

Enquiries about DBS Data Protection Policy should be addressed to The Data Controller.

4.2. Fair Obtaining and Processing

DBS undertakes to obtain and process data fairly and lawfully by informing all data subjects of the reasons for data collection, the purposes for which the data are held, the likely recipients of the data and the data subjects' right of access. Information about the use of personal data must be printed on the appropriate collection form. If details are given verbally, the person collecting must explain the issues before obtaining the information.

5. Data Integrity

DBS undertakes to ensure data integrity by the following methods:

5.1 Data Accuracy

Data held will be as accurate and up to date as is reasonably possible. If a data subject informs DBS of a change of circumstances their records will be updated as soon as is practicable. DBS will ensure that a regular process of validation and accuracy checking is undertaken.

In circumstances where a data subject challenges the accuracy of their data, DBS will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to

resolve the issue informally, but if this proves impossible, disputes will be referred to the DBS Board of Governors. If the problem cannot be resolved at this stage, either side may seek independent arbitration. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

5.2 Data Adequacy and Relevance

Data held about people will be adequate, relevant and not excessive in relation to the purpose for which the data is being held. In order to ensure compliance with this principle, DBS will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data.

5.3 Length of Time

Data held about individuals will not be kept for longer than necessary for the purposes registered. It is the duty of the nominated person to ensure that obsolete data is properly erased in accordance with the DBS Information Management.

6. Subject Access

6.1 General

The Law No. 13/2016 concerning Privacy and Protection of Personal Data extends to all data subjects the right of access to their own personal data. In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place.

Where a request for subject access is received from a student, the DBS policy is that:

Requests from students will be processed as any subject access request as outlined below and the copy will be given directly to the student, unless it is clear that the student does not understand the nature of the request.

Requests from students who do not appear to understand the nature of the request will be referred to their parents. Requests from parents in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the copy will be sent in a sealed envelope to the requesting parent only after the appropriate checks have been carried out to ensure that the requesting person is allowed access to that information.

6.2. Processing subject access requests

Students, parents or staff may request information by submitting a written request with the Principal's Personal Assistant. Provided that there is sufficient information to process the request, an entry will be logged, showing the date of receipt, the data subject's name, the name and address of requester (if different), the type of data required (e.g. Student Record, Personnel Record), and the planned date of supplying the information (normally not more than 40 days from the request date). Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the date of entry in the log will be dated on which sufficient information has been provided.

Note: In the case of any written request from a parent regarding their own child's record, access to the record will be provided within two weeks of the request.

6.3. Data Processors

i. DBS may use third party data processors to process personal data on its behalf but where this is done responsibility for compliance with the Data Protection Principles remains with DBS. In order to ensure that any data processors own practices are compliant DBS will:
ii. Check any Data Processors Data Protection Registration in its country of operation prior to commencement of negotiations. Review the Data Processors own Data Protection Policy and Procedures to ensure that they are compliant with DBS own policies.
iii. DBS will reserve the right to inspect the Data Processors records at any time to ensure that they are compliant.

In the event of a breach or a suspected breach of the contract terms and regulatory requirements the DBS will:

iv. Take immediate action to limit the breach including withdrawing all permissions to process data from the Data Processor and suspension of the agreement.
v. Carry out and document a risk assessment to identify the potential adverse consequences of the breach for individuals; how serious or substantial these are; and how likely they are to happen.
vi. Inform any person or organisation that may be affected by the breach, including but not limited to: individuals affected, MOEHE, Child Protection Agencies, Banks and police.
vii. Consult with its Public Relations advisors and consider how to respond to any media enquiries related to the breach.

7. Authorised Disclosures

DBS will, in general, only disclose data about individuals with their consent. However, there are circumstances under which the DBS is authorised to disclose data without explicit consent for that occasion.

These circumstances are strictly limited to:

i. Student data disclosed to authorised recipients related to education and administration necessary for DBS to perform its obligations as an educational establishment.
ii. Student data disclosed to authorised recipients in respect of their child's health, safety and welfare.
iii. Student data disclosed to parents in respect of their child's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of DBS.
iv. Staff data disclosed to relevant authorities e.g. in respect of payroll and administrative matters.
v. Unavoidable disclosures, for example to an engineer during maintenance of the computer system. In such circumstances the engineer would be required to sign a form promising not to disclose the data outside DBS.

vi. Only authorised and trained staff are allowed to make external disclosures of personal data. Data used within DBS by administrative staff and teachers will only be made available where the person requesting the information is a professional legitimately working within the school who **need to know** the information in order to do their work. DBS will not disclose anything on students' records which would be likely to cause serious harm to their physical or mental health or that of anyone else – including anything where suggests that they are, or have been, either the subject of or at risk of child abuse.

A "legal disclosure" is the release of personal information from the computer to someone who requires the information to do his or her job within or for DBS, provided that the purpose of that information has been registered. An "illegal disclosure" is the release of information to someone who does not need it, or has no right to it, or one which falls outside the DBS registered purposes.

8. Data and Computer Security

DBS undertakes to ensure security of personal data by the following general methods (precise details cannot, of course, be revealed) and by adherence to internal security policies.

9. Physical Security

Appropriate building security measures are in place, such as alarms, deadlocks and computer hardware cable locks. Only authorised persons are allowed in the server room. Disks, tapes and printouts are locked away securely when not in use. Visitors to DBS campuses are required to sign in and out, to wear identification badges whilst in the school and are, where appropriate, accompanied all in accordance with DBS Security Policy.

10. Logical Security

Security software is installed on all computers containing personal data. Only authorised users are allowed access to the computer files and password changes are regularly undertaken. Computer files are backed up (i.e. security copies are taken) regularly, all in accordance with the DBS Policy.

11. Procedural Security

In order to be given authorised access to the computer, staff will have to undergo checks and will sign a confidentiality agreement. All staff are trained in their Data Protection obligations and their knowledge updated as necessary.

Any documents with confidential information will be disposed of in accordance with the DBS Information Management Policy.

The security policies are determined by the Director of Education and is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent.

Any queries or concerns about security of data at first should in the first instance be referred to the Principal.

Individual members of staff can be personally liable in law under the terms of the Law No. 13/2016.

APPENDIX 1

Access to Personal Data Request (Under Law No. 13/2016 concerning Privacy and Protection of Personal Data)

Name:

Address:

Telephone Number:

Are you the person who is the subject of the records you are enquiring about **YES / NO**
If NO,

Do you have parental responsibility for a child who is the "Data Subject" of the **YES / NO**
If YES,
Name of student or students about whose personal data records you are enquiring
1)
2)
3)
Description of Concern / Area of Concern

Description of Information or Topic(s) Requested

Additional information. Please despatch Reply to: (if different from enquirer's details as stated on this form)
Name:
Address:
Postcode:

Data Subject Declaration
I request that DBS search its records based on the information supplied above and provide a description of the personal data found from the information described in the details outlined above relating to me (or my child/children) being processed by the school. I agree that the reply period will commence when I have supplied sufficient information to enable the school to perform the search.
I consent to the reply being disclosed and sent to me at my stated address (or to the Despatch Name and Address above who I have authorised to receive such information).

Signature of "Data Subject" (or Subject's Parent) …….

Name of "Data Subject" (or Subject's Parent) (PRINTED)…….

Dated …….


Thank you