# DATA PROTECTION POLICY

## W52

| | |
|---|---|
| **Policy owner:** | **Head of IT Systems** |
| **Policy agreed on:** | **September 2016** |
| **Policy reviewed on:** | **November 2023** |
| **Policy to be reviewed on:** | **November 2025** |

## DOCUMENT CONTROL TABLE

| | | |
|---|---|---|
| **Status** | | **LIVE** |
| **Policy owner** | | **Head of IT Systems** |
| **Statutory/Recommended** | | **STATUTORY** |
| **Date approved** | | **SEPTEMBER 2019** |
| **Review period** | | **2YEARS** |
| **Latest review date** | | **November 2023** |
| **Revision** | | **November 2025** |
| **Linked documents and policies** | | **COMPLAINTS POLICY**<br><br>**SAFEGUARDING AND CHILD PROTECTION POLICY** |
| **Version** | **Date** | **Comments** |
| **1.1** | **November 2023** | **Changed DPO to Head of IT systems** |

## TERMINOLOGY

| | |
|---|---|
| **Personal Data** | Any information relating to an identified, or identifiable, living individual.<br><br>This may include the individual's:<br><br>• Name (including initials)<br>• Identification number<br>• Location data<br>• Online identifier, such as a username<br><br>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural, or social identity. |
| **Special categories of personal data** | Personal data, which is more sensitive and so needs more protection, including information about an individual's:<br><br>• Racial or ethnic origin<br>• Political opinions<br>• Religious or philosophical beliefs<br>• Trade union membership<br>• Genetics<br>• Biometrics (such as fingerprints, retina, and iris patterns), where used for identification purposes<br>• Health – physical or mental |
| **Processing** | Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing, or destroying. Processing can be automated or manual. |
| **Data subject** | The identified or identifiable individual whose personal data is held or processed. |
| **Data protection officer (DPO)** | This person will monitor observance of the principles of this policy. The data protection officer will also act as the contact point for any access requests. |

| | |
|---|---|
| **Data processor** | A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller. |
| **Personal data breach** | A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. |
| **Data controller** | A person or organisation (the school) that determines the purposes and the means of processing of personal data. |

## CONTENTS


Overview 5

Purpose 5

Roles and Responsibilities 5

Data Protection Principles 6

General Statement 7

Sharing Personal Data 7

Subject Access Requests and other Rights of Individuals 8

Children and Subject Access Requests 9

Responding to Subject Access Requests 9

Other Data Protection Rights of the Individual 10

Data Security and Storage of Records 10

Disposal of Records 11

Personal Data Breaches 12

Complaints 12

Appendix 1 – Personal Data Breach Procedure 12

## OVERVIEW

Doha College uses personal information about staff, pupils, parents, and other individuals who come into contact with the school.
This information is gathered to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use the information to ensure that the school complies with its statutory obligations.

## PURPOSE

This policy is intended to ensure that personal information is dealt with correctly and securely and following the Data Protection Act 1998 and other related legislation. It will apply to information regardless of how it is collected, used, recorded, stored, and destroyed and whether it is held in paper files or electronically.

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

## ROLES AND RESPONSIBILITIES

This policy applies to **all staff** employed by our school and external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

### Governing board

The governing board ensures that our school complies with all relevant data protection obligations.

### Principal

The Principal acts as the representative of the data controller on a day-to-day basis.

### Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

The DPO will share with the leadership and the board if there are any breaches to our data protection policy.
The DPO is also the first point of contact for individuals whose data the school processes.
Full details of the DPO's responsibilities are set out in their job description.

Our DPO is **David Lish** and is contactable via **systems@dohacollege.com**

### All staff

Staff are responsible for:

Collecting, storing, and processing any personal data following this policy
Informing the school of any changes to their data, such as a change of address
Contacting the DPO in the following circumstances:

- With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure.
- If they have any concerns that this policy is not being followed
- If they are unsure whether or not, they have a lawful basis for using personal data in a particular way
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data.
- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

## DATA PROTECTION PRINCIPLES

The *Data Protection Act 1998,* the *EU General Data Protection Regulation (GDPR) 2018*, and Qatar Law No. 13 of 2016 on Protecting Personal Data Privacy establishes enforceable principles that will be adhered to:

- Personal data shall be processed fairly and lawfully;
- Personal data shall be obtained only for one or more specified and lawful purposes;
- Personal data shall be adequate, relevant, and not excessive;
- Personal data shall be accurate and, where necessary, kept up to date;
- Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;
- Personal data shall be kept secure, i.e., protected by an appropriate degree of security;

- Consent must be obtained to hold personal data; it cannot be assumed; consent must be clear and distinguishable from other matters, provided in an intelligible and easily accessible form using clear and plain language;
- Individuals have the right to request a copy of the data held about them or to have such data erased;
- Any data breach should be notified to the regulatory authorities within 72 hours.

## GENERAL STATEMENT

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

- Inform individuals why the information is being collected and 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 aware of and understand our policies and procedures

## SHARING PERSONAL DATA

We will not usually share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk.
- There is a safeguarding concern.

- We need to liaise with other agencies to protect the child.
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law.
- Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service.
- We will also share personal data with law enforcement and government bodies where we are legally required to do so.
- We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.
- When we transfer personal data locally or internationally, such as to a new school, we will do so following data protection law.

## SUBJECT ACCESS REQUESTS AND OTHER RIGHTS OF INDIVIDUALS

### Subject access requests

- Individuals have a right to make a 'subject access request' to access personal information that the school holds about them. This includes:
- Confirmation that their data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long will the data be stored for, or if this isn't possible, the criteria used to determine this period

Where relevant, the existence of the right to request rectification, erasure, or restriction or to object to such processing.

- The source of the data, if not the individual

- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally
- Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include the following:
- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested.
- If staff receive a subject access request, they must immediately forward it to the DPO.

## CHILDREN AND SUBJECT ACCESS REQUESTS

Personal data about a child belongs to that child and not the child's parents or carers. For a parent or carer to make a subject access request for their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children below the age of 12 are generally not considered mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule, and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Children aged 12 and above are generally mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

## RESPONDING TO SUBJECT ACCESS REQUESTS

When responding to requests, we:

- May ask the individual to provide two forms of identification.
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within one month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)

- Will provide the information free of charge
- May tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month and explain why the extension is necessary.
- We may not disclose information for a variety of reasons, such as if it:
- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's data that we can't reasonably anonymise, and we don't have the other person's consent, and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts
- If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will consider whether the request is repetitive when making this decision.

When we refuse a request, we will tell the individual why, and they have the right to make a complaint.

## OTHER DATA PROTECTION RIGHTS OF THE INDIVIDUAL

In addition to the right to make a subject access request (see above) and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- Withdraw their consent to the processing at any time
- Ask us to rectify, erase or restrict the processing of their data (in certain circumstances)
- Prevent the use of their data for direct marketing
- Object to processing which has been justified based on public interest, official authority, or legitimate interests
- Challenge decisions based solely on automated decision-making or profiling (i.e., making decisions or evaluating certain things about an individual based on their data with no human involvement)

- Be notified of a data breach (in certain circumstances)
- Ask for their data to be transferred to a third party in a structured, commonly used, and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

## DATA SECURITY AND STORAGE OF RECORDS

We will protect personal data and keep it safe from unauthorised access, alteration, processing, or disclosure and against accidental or unlawful loss, destruction, or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or went anywhere else where there is general access
- Where personal information needs to be taken off-site, staff must sign it in and out from the school office
- Passwords at least eight characters long containing letters and numbers are used to access school computers, laptops, and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites or share passwords
- Staff, pupils, or governors who store personal information on their devices are expected to follow the same security procedures as for school-owned equipment
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected

## DISPOSAL OF RECORDS

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or outdated will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records and overwrite or delete electronic files. We may also use a third party to dispose of records on the school's behalf safely. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

## PERSONAL DATA BREACHES

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure in appendix 1.

## COMPLAINTS

Complaints will be dealt with following the school's complaints policy.

## APPENDIX 1 PERSONAL DATA BREACH PROCEDURE

This procedure is based on **guidance on personal data breaches** produced by the Information Commissioner's Office (ICO).

On finding or causing a breach, or potential violation, the staff member, governor, or data processor must immediately notify the data protection officer (DPO). The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people

Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation.

If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the Principal and the chair of governors

The DPO will make all reasonable efforts to contain and minimise the breach's impact. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g., from IT providers).

The DPO will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences.

The DPO will document the decisions (either way) in case the decisions are challenged at a later date.

*Where the Information Commissioner's Office (ICO) must be notified, the DPO will do this via the 'report a breach' page of the ICO website or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. As required, the DPO will set out:*

A description of the nature of the personal data breach, including, where possible:

- The categories and approximate number of individuals concerned
- The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach

- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the school's awareness of the breach. The report will explain why there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining data as soon as possible

Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:

- A description, in clear and plain language, of the nature of the personal data breach
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.

The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.

The DPO will document each breach, irrespective of whether it is reported to the ICO. For each violation, this record will include the following:

- Facts and cause
- Effects
- Action is taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

The DPO and Principal will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

The DPO and Principal will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches.

Actions to minimise the impact of data breaches on staff

*Sensitive information being disclosed via email (including safeguarding records)*

If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error

Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error

If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the [ICT department/external IT support provider] to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence)

In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the data and do not share, publish, save, or replicate it in any way.

The DPO will endeavour to obtain a written response from all the individuals who received the data, confirming that they have complied with this request.

The DPO supported by the Head of Communications, will carry out an internet search to check that the information has not been made public; if it has, they will contact the publisher/website owner or administrator to request that the data is removed from their website and deleted.

If safeguarding information is compromised, the DPO will inform the executive designated safeguarding lead.

*Other examples of data breaches that staff must report may include:*

Details of interventions for named children are being published on the school website

Non-anonymised pupil exam results or staff pay information being shared with governors

A school laptop containing non-encrypted sensitive personal data being stolen or hacked

The school's cashless payment provider is being hacked, and parents' financial details stolen

Hardcopy reports sent to the wrong pupils or families

# DOHA COLLEGE

Accredited by

BSME | Accredited Member
BRITISH SCHOOLS IN THE MIDDLE EAST

British School Overseas BSO Inspected

CIS WE ARE AN ACCREDITED SCHOOL

The Patron's ACCREDITATION AND COMPLIANCE ACCREDITED

HPL Membership Network

Eco-Schools

## About Doha College

**Vision**

To enable personal growth, instil a passion for learning and create aspirational minds.

**Mission**

With the growth-mindset philosophy of High Performance Learning, we develop confidence, creativity and intellectual curiosity in a safe, caring and inclusive environment for our students to make a lasting contribution to global society.

**Core Values**

Excellence and diligence
Respect and Integrity
Commitment and Accountability
Perseverance and Honesty
Fun and Enjoyment
Challenge and reward

**Doha College**
PO Box 7506,
Doha, State of Qatar

+974 4407 6777
enquiries@dohacollege.com
www.dohacollege.com

A BRITISH INTERNATIONAL SCHOOL