

Quwwat-ul-Islam Girls' School



Data Protection Policy

Published Date	September 2026
Review Date	July 2027
Policy Links	Confidentiality Policy Data retention and destruction Policy

School Motto
Together we can achieve more
School Values
Respect . Aspiration . Responsibility
Learning Drivers
Caring for Ourselves, Our World, Our Education, Our Rights

School Vision Statement

To establish a school of excellence both **Islamically** and **Academically** - Provide a **holistic** education which is inspired by: **Taqwa**: God consciousness **morals and values** inspired by the prophet (saw) coupled with **academic excellence**.

At Quwwat-ul-Islam girls' school we adhere to the following:

- **Mutual respect and tolerance** - We respect and care for everybody.
- **Democracy**– We promote the right of every individual to have their opinions and voices heard.
- **The rule of the law** – We understand that laws and rules protect us and at the same time provide us with responsibilities, by breaking them there are consequences.

Quwwat ul Islam Girls' School is committed to safeguarding and promoting the welfare of all pupils in its care. As an employer, the school expects all staff, governors, volunteers and parents/carers to share this commitment.

Introduction

This Data Protection Policy regulates and details the way in which Quwwatul Islam Girls' School obtains, uses, holds, transfers and processes Personal Data and Sensitive Personal Data about individuals and ensures that all School employees know the rules for protecting Personal Data.

This Policy also describes individuals' rights in relation to their Personal Data processed by the school.

The school has practices in place in relation to their handling of Personal Data to ensure that they are acting in accordance with UK laws and other relevant regulatory guidance. The most notable legislation in this area is the General Data Protection Regulation (GDPR).

The school shall comply with the principles of the GDPR to ensure that all data is:

- ☐ Fairly and lawfully processed
- ☐ Processed only for lawful purposes
- ☐ Adequate, relevant, and not excessive
- ☐ Accurate and up to date
- ☐ Not kept for longer than is necessary
- ☐ Processed in accordance with the data subject's rights
- ☐ Secure
- ☐ Not transferred to other countries without consent and adequate protection

In addition, the school will also comply with the GDPR that introduces further rights for individuals and strengthens some of the rights already in existence under the previous data protection act:

- ☐ The right to be informed
- ☐ The right of access
- ☐ The right to rectification
- ☐ The right to erasure
- ☐ The right to restrict processing

- ☐ The right to data portability
- ☐ The right to object
- ☐ Rights in relation to automated decision making and profiling

At all times, the school will endeavour to ensure that it has a legal basis for the processing of personal information.

Quwwat Ul Islam Girls' School is registered as a Data Controller with the Information Commissioner's Office (ICO). Our registration number is **ZA477381**

Personal Data

"Personal Data" is any information (for example, a person's name) or combination of information about a living person (such as name and address and date of birth) which allows that living person to be identified from that information and which relates to them, such as the job application of "Aisha Ahmed" with her address and date of birth, or the academic record of "Aisha Ahmed" with similar details. If in doubt, individual details should be treated as Personal Data.

Examples of Personal Data which may be used by the school in its day-to-day business include employee, pupil, parent details, such as names, addresses, telephone numbers and other contact details, such as email addresses and mobile numbers, CVs, performance reviews, photos, payroll and salary information. This could affect job applicants, direct employees, temporary staff, volunteers, parents, pupils, individual consultants or contractors, visitors etc.

The definition of Personal Data also includes opinions about a person and appraisals about or statements of intent regarding them.

The laws governing how the school can use Personal Data apply whether the Personal Data is stored electronically (for example, in emails, on IT systems, as part of a database or in a word-processed document) or in structured paper records (for example, in paper files, card indexes or filing cabinets).

Processing of Personal Data & Audits

The school uses or processes Personal Data (including Sensitive Personal Data, see section 7) on a range of individuals for a multitude of business purposes, including the use of CCTV systems. Such individuals may include staff and contractors, pupils and parents, business contacts, job applicants and former employees, and the person whose Personal Data is used by the school is known as **"the data subject"**.

When the School collects, stores, uses, discloses, updates, or deletes or destroys Personal Data, this is called “processing”. All processing is regulated by data protection legislation and must meet certain conditions to be carried out lawfully.

The school maintains a database of personal data with clear retention schedules and the Office Manager conducts regular audits of Personal Data held.

Personal Data and Sensitive Personal Data are held securely by the school and staff are regularly briefed by the SLT and via the ICT policies on appropriate and safe data management.

Legislation and Information Commissioner’s Office

Data protection laws are enforced in most countries by the local Data Protection Authority, in the UK being the Information Commissioner’s Office (“the “ICO”). The ICO may investigate concerns and complaints, may audit the school’s use or processing of Personal Data, and may take action against the school for breach of these laws.

Action may include making the school pay a fine and/or stopping the use by the School of the Personal Data, which may prevent it from carrying on its business. There is also the risk of negative publicity.

In addition, the General Data Protection Regulation (GDPR) introduces more stringent data protection obligations on Data Controllers.

Transparency and Personal Data

The school is entrusted to use the Personal Data of individuals on the basis that the proposed use is transparent, expected and clearly defined. Accordingly, one of the main data protection obligations requires the school to process Personal Data fairly.

In addition, use of Personal Data must be lawful. In practice, this means that the school will comply with at least one of the following conditions when processing Personal Data:

- ☐ The individual to whom the Personal Data relates has consented to the processing.
- ☐ The processing is necessary for the performance of a contract between the school and the individual (or to enter into that contract at the individual’s request)

- ☐ The processing is necessary to comply with a legal obligation (not a contractual obligation) placed on the school.
- ☐ The processing is necessary to protect a vital interest of the individual (where there is an imminent risk to their life or of serious harm to them otherwise); or
- ☐ The processing is necessary to pursue the legitimate interest of the school (or proposed recipient of the Personal Data) but where on balance; this would not involve disproportionate harm to the individual.

Use of Personal Data should meet one or more of these conditions. If there are any concerns about this; it is proposed to use Personal Data for additional purposes; or new reasons for using Personal Data are contemplated, reliance on these conditions must be discussed in the first instance with the Office Manager prior to being relied upon.

All new Personal Data processing activities and projects involving the use of Personal Data must be approved prior to being started as there are complex exemptions and other lawful reasons for processing which may apply. For example, if someone provides their details as a contact, you will not be able to start sending them marketing emails unless that is covered in an appropriate notice and consent from that individual.

In addition, the school ensures its Personal Data is accurate and up to date. The school takes care to record and input Personal Data accurately. Some Personal Data may change from time to time (such as addresses and contact details, bank accounts). It is important to keep current records up to date. The school takes care to update records promptly and correctly.

Privacy Notices

When an individual provides the school with any Personal Data about themselves, the school will make sure the individual knows:

- ☐ who is responsible for the Processing of their Personal Data;
- ☐ for what purposes that the school will process the Personal Data provided to it.
- ☐ sufficient details about any proposed disclosures/transfers of their Personal Data to Third Parties (including any cross-border transfers);
- ☐ the rights that the individual has in respect of their personal data.

- ☐ any other information that the individual should receive to ensure the processing carried out is within his/her reasonable expectations (retention periods for instance); and
- ☐ who to contact to discuss or raise any Personal Data issues.

The school does this by providing this information and it is known as providing a “privacy notice” or fair processing notice. Before collecting Personal Data, staff at the school will give individuals providing those details appropriate Privacy Notices, these may be embedded in contracts, or on websites or form part of application or other forms. The school will inform individuals about the processing of their Personal Data before or at the time the data is collected. The information contained in its Privacy Notices will be concise and easily accessible and written in clear and plain language.

The school will only process Personal Data in a manner and for purposes consistent with the relevant privacy notice(s) already provided to an individual. Personal Data should not be collected for one purpose and then used for a second purpose unless that is also set out in the relevant notice.

Sensitive Personal Data

“Sensitive Personal Data” (or “**Special Category**”) is personal Data about a person’s race or ethnicity, their health, their sexual preference, the medical information, their religious beliefs, their political views, trade union membership or information accusing an individual of any crime, or about any criminal prosecution against them, and the decision of the court and any punishment.

The Office Manager can provide further information on what is, and the handling of, Sensitive Personal Data. Sensitive Personal Data should not be collected or used unless essential. It must be treated as strictly confidential. Extra care must be taken with it and it must be kept more securely. In addition to the normal requirements for lawful use of any Personal Data such details should not be used without the explicit prior consent of the individual, which has to be clear, unambiguous and voluntary.

- ☐ The school does not seek to obtain Sensitive Personal Data unless:
- ☐ the individual concerned agrees in writing that we may do so, on the basis of a full understanding of why the school is collecting the data
- ☐ the school needs to do so to meet its obligations or exercise its rights under any relevant laws
- ☐ in circumstances such as where the processing is necessary to either safeguard or protect the vital interests of the individual concerned

Sensitive Personal Data should not be disclosed unless measures are taken to encrypt or otherwise secure that information due to the potential for harm or distress if the email is received by unintended recipients or otherwise goes astray.

Sensitive Personal Data should be collected and used as little as possible and be subject to more limited and strictly needed access and used subject to greater security measures than other Personal Data.

Other Personal Data where misuse may lead to distress or harm, especially to fraud or identity theft (for example, bank account or credit card details, or official government identification numbers, such as national insurance contribution numbers) must be treated like Sensitive Personal Data.

Employee Obligations

All School staff should be aware of their obligations and comply at all times with this Policy.

All staff must ensure that Personal Data collected by them must be appropriate to and sufficient for the relevant purpose(s) for which it is collected but not excessive for that purpose(s). Use of Personal Data should be minimised and not maximised. Collecting unnecessary personal Data adds to the school's compliance burden.

Where staff are dealing with pupil and parent data already collected by the school, the individual/s concerned will have given consent on joining the school for the processing of their personal data for the purposes of running the school.

All staff involved in the processing of personal information will:

- ☐ Read and understand this policy
- ☐ Use strong passwords
- ☐ Encrypt all portable devices if they contain personal data
- ☐ Only keep information as long as necessary
- ☐ Staff should not download personal data onto personally owned devices unless absolutely necessary. In such cases, the personal data should be deleted from the personal device as soon as is practicable after use.

Data retention & School Archives

Site Transition Register

The school maintains daily AM and PM attendance registers on the electronic system. In addition, a Site Transition Register must be used to record students moving between buildings during the school day. This register will be kept in a dedicated logbook and retained for the duration of each term.

At the end of each term, the logbook will be securely disposed of in line with school data management procedures. Previous term registers are not retained to reduce the risk of unnecessary data storage, support efficient record management, and ensure compliance with data protection principles by only keeping information for as long as it is operationally required.

Personal Data must be stored securely and will be kept in accordance with the Data Retention Policy. Some records have to be retained for minimum periods by law (such as records on employee payments and their taxation under tax laws).

As a general rule, when Personal Data is no longer needed for the purposes for which it was collected, this Personal Data will be securely and permanently destroyed as soon as practicable.

The school will not delete or destroy or amend records containing Personal Data without explicit consent once they have been informed those records have been requested by the individual whose Personal Data it is, or by a Data Protection Authority. Such a breach may be a criminal offence with personal liability.

The Right to Information, the Right to Erasure and Subject Access Requests

Individuals have certain rights in relation to their Personal Data:

- ☐ The right to obtain information (what Personal Data, from where, used for what purposes and shared with which recipients) about Personal Data held about themselves and to obtain copies of such Personal Data (Subject Access Request).
- ☐ The right to prevent processing of Personal Data for direct marketing purposes.
- ☐ The right to object to and stop certain processing of Personal Data where it is likely to cause substantial unwarranted harm or distress
- ☐ The right to have Personal Data corrected
- ☐ The right to compensation for any damage/distress suffered from any breach.
- ☐ The right to be informed of automated decisions made about them.

If any member of School staff receives such a request or demand from an individual, they must promptly inform the Office Manager

Individuals are also allowed to withdraw their consent (where this is not required for the school's legitimate interests) to the school's use of their Personal Data at any time. If a school employee receives such a withdrawal of consent, they must promptly inform the Office Manager

If anyone at the school receives a request to stop sending marketing materials, direct marketing communications of that type to that individual must be stopped as soon as possible.

Individuals can also ask in writing for copies of their Personal Data which the school holds about them and other details about how the school uses their Personal Data.

Subject to receipt of proof of ID were considered necessary (and payment of any official fee permitted which the school has requested), following receipt of a written request from an individual for access to his/her Personal Data, the school will (to the extent requested by the individual):

- ☐ inform that individual whether the school holds Personal Data about him or her.
- ☐ describe the Personal Data about the individual which it holds,
- ☐ the reason for holding the Personal Data and the categories of persons to whom it may disclose the Personal Data; and
- ☐ provide the individual with copies of the Personal Data held about him or her, together with an indication of the source(s) of the Personal Data.

Strict rules must be followed as part of this process. Therefore, any such request received should be passed on to the Office Manager. There are strict statutory deadlines for responding. School staff must not respond to any such request directly.

There is a right under the DPA known as “the right to be forgotten”. This gives an individual the right to have their data erased when there is no compelling reason for continued processing. Under the DPA, the right to erasure is limited to processing that causes unwarranted and substantial damage or distress. Under the GDPR, this test is not present. However, if the processing does cause damage or distress, this is likely to make the case for erasure stronger.

Data Security

The school endeavours to keep all Personal Data secure by protecting data against being accessed by other companies or individuals (for example, via hacking), from being corrupted (data corruption) or being lost or stolen. This applies to Personal Data in IT systems, emails and attachments and paper files.

School staff must comply with the school’s security procedures whenever processing Personal Data. The school is dependent upon all employees to help keep Personal Data secure. Employees must only access and use Personal Data they are individually authorised to access and use, and which is needed for a specific task within their school role.

School employees who work away from the school's premises must comply with any additional procedures and guidelines issued by the school for home working and/or offsite working. Extra care is needed to secure Personal Data in such cases, particularly Sensitive Personal Data.

The school also recognises that adequate security is important where it arranges for Third Parties to process Personal Data on its behalf, such as when outsourcing services to service providers, who process Personal Data on behalf of the school as a result ("a Data Processor"). The school remains liable for those service providers and their treatment of the Personal Data. The school will have suitable written contracts in place with such service providers with specific terms included to protect the Personal Data provided to them.

Data Security

Disclosing Personal Data to Third Parties and Overseas Transfers

A disclosure of Personal Data is a form of processing. That means that the rules described above for fair and lawful use have to be satisfied. The school will not disclose Personal Data to a Third Party without first checking the disclosure is lawful and proportionate.

There are some exceptions to deal with disclosures, such as those requested lawfully by police where the information is necessary to prevent or detect a crime. Any request for Personal Data about an individual from government, police or other similar bodies or from journalists or other investigators should be passed immediately to the Office Manager.

From time to time the school may pass pupil personal data (including sensitive personal data where appropriate) to third parties where lawful to do so, including local authorities, other public authorities, health professionals, the data will be used:

- ☐ to enable the relevant authorities to monitor the school's performance.
- ☐ to compile statistical information (normally used on an anonymous basis).
- ☐ to safeguard pupils' welfare and provide appropriate pastoral (and where relevant, medical and dental) care for pupils.
- ☐ where specifically requested by pupils and/or their parents or guardians.
- ☐ where necessary in connection with learning and extra-curricular activities undertaken by pupils.
- ☐ to enable pupils to take part in national and other assessments and to monitor pupils' progress and educational needs.
- ☐ to obtain appropriate professional advice and insurance for the school.
- ☐ where a reference or other information about a pupil or ex-pupil is requested by another educational establishment or employer to whom they have applied, otherwise where reasonably necessary for the operation of the school.

Unlawful disclosure (however well-meaning and however seemingly authoritative the requestor) risks placing the school in breach of several obligations under data protection legislation. Special care is needed with telephone requests for information, often used by unauthorised parties to 'blag' or obtain Personal Data to which they are not entitled. School employees must be certain of the identity of the person with whom they are dealing, ideally have a written request for information from them and ensure any disclosures are justified and authorised in advance.

There are special rules on whether Personal Data can be transferred to another country. Within the EU, there are restrictions on the transfer of Personal Data outside of the European Economic Area (EEA) (such a transfer can happen, for example, where Personal Data is emailed outside the EEA; where the School IT servers are hosted outside the EEA; or where there is remote on-screen access from outside the EEA to Personal Data stored in an IT system within the EEA). This is to make sure the Personal Data remains safeguarded and that the individuals concerned do not lose the protection and rights they have under local law in respect of their Personal Data when transferred.

Actual or likely transfers of Personal Data to outside the EEA, especially of Sensitive Personal Data, should be clearly set out in the privacy notices described in the fair use section of this Policy above so that such transfers are expected by the affected individuals.

Club, Alumni, Marketing and Fundraising

As with other types of Processing, the use of Personal Data for marketing and fundraising purposes must satisfy the fair and lawful use requirements set out above. This means information notices must be given, and a lawful reason for processing has to be satisfied. Typically, this will have to be consent based.

Personal Data should not be used to contact individuals for marketing purposes by email, text or similar unless the individual has consented to marketing use. Individuals have a right to decline postal marketing and to object to any fundraising. Where marketing or fundraising is to be by phone, email, text or similar electronic means, normally individual consent is needed and must clearly cover marketing by that communication method. Special rules apply as to when consent is needed.

Appendix 1.

Key Summary and Top Tips for School Staff Data Protection

Background

80% of data breaches involve staff within an organisation (figure from the Information Commissioner's Office) and breaches, for the most part, are unintentional. Therefore, everyone dealing with Personal Data needs to have a basic understanding of the Data Protection Act 1998 (DPA) and the new General Data Protection Regulations (coming into force in May 2018) that introduces more stringent data obligations.

The school collects a variety of personal data on students, parents, alumni, contractors, staff, volunteers, business contacts etc. for legitimate business reasons in connection with the running of the school. It is vital that all this information is kept securely, is regularly reviewed and disposed of when no longer required.

Top Data Protection Tips:

- ☐ Read and follow the School's Data Protection Policy
- ☐ Make sure all new staff within your department are aware of the school's policy and any departmental procedures regarding data protection
- ☐ Use strong passwords on all devices and two step authentications wherever possible. Ensure that any device you access school personal data on (mobiles for instance) are password protected.
- ☐ Do not download personal data onto personally owned devices or send email to home email addresses unless absolutely necessary. In such cases, any personal data should be permanently deleted from the personal device as soon as possible after use. Use Google Drive when working from home/ remote teaching
- ☐ Only keep information as long as necessary - conduct periodic reviews (at least yearly) of personal systems (paper and electronic) and delete personal data that is no longer required.
- ☐ Remember that most data breaches are unintentional - double check who you are sending information to, don't leave computers unattended and unlocked and make sure you shred confidential information when it is no longer required.
- ☐ Before sharing any personal information (this includes photos), check the school has the relevant permission to do so.

Tips on keeping information secure:

- ☐ Keep passwords secure – change these regularly and do not share or give other people your password. Use two step authentications.
- ☐ Always lock / log off computers when away from your desk
- ☐ Dispose of confidential paper waste securely by shredding
- ☐ Prevent virus attacks by taking care when opening emails and attachments or visiting new websites
- ☐ Hard copy personal information should be stored securely when it is not being used (lockable cabinets etc.).
- ☐ Be careful when discussing individuals that you are not in earshot of anyone who does not need access to that information
- ☐ Position computer screens away from windows and walkways to prevent accidental disclosures of personal information
- ☐ Encrypt personal information that is being taken or sent outside the school or office.
- ☐ Do not, unless absolutely necessary, download personal data to a non-school device.

Tips on keeping only relevant information:

- ☐ Collect only the personal information required
- ☐ Explain new or changed business purposes to parents, pupils, employees, and others, and obtain consent or provide an opt-out or opt-in where appropriate.
- ☐ Update records promptly – for example, changes of address, phone numbers.
- ☐ Delete personal information the school no longer requires. If in doubt, please check whether the information should be retained. In the case of safeguarding information, this should always be passed to the Designated Safeguarding Lead to decide whether or not the information should be retained.
- ☐ Be aware that there may be people who will try and trick staff into giving out personal information
- ☐ Carry out identity checks before giving out personal information to anyone in person, by writing or over the phone.