Data Protection and GDPR Policy

Introduction

We are committed to protecting the privacy and security of all personal information we collect. This policy explains how we collect, use, store, and share personal data in line with the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

Purpose of this Policy

This policy aims to:

- Follow UK GDPR and the Data Protection Act 2018.
- Protect the personal data of students, parents, staff, and other stakeholders.
- Be clear about how we collect, use, and share data.
- Promote transparency and responsibility in handling data.

Who this Policy Covers

This policy applies to personal data held by the Madrasah about:

- Students and their families.
- Staff, volunteers, and contractors.
- Trustees and other related individuals.

It covers both paper and digital records.

Data Protection Principles

We follow the seven key GDPR principles when handling personal data:

1. Lawful and transparent – We collect data legally and explain clearly why we need it.
2. Limited use – We use data only for the reasons it was collected.
3. Data minimisation – We only collect what we need.
4. Accuracy – We keep data up-to-date.
5. Storage limits – We only keep data for as long as necessary.
6. Security – We keep data safe from loss or misuse.
7. Accountability – We keep clear records and follow proper procedures.

Types of Data We Collect

We may collect:

- Personal details (name, date of birth, address, contact info).
- Education records (attendance, progress).
- Medical details (allergies, health needs, emergency contacts).
- Safeguarding information (e.g., court orders).
- Staff data (qualifications, payroll details).

Why We Collect Pupil Information

We collect pupil information to:

- Support learning and development.
- Track and report on progress.
- Monitor teaching quality.
- Keep pupils safe (e.g., allergy info).
- Meet legal requirements.
- Protect children's welfare.

Legal Reasons for Processing Data

We process data based on:

- Consent – e.g., permission to use photos.
- Contract – e.g., for staff employment.
- Legal obligation – e.g., for safeguarding.
- Legitimate interest – e.g., for day-to-day operations.

Subject Access Rights

Parents and carers have the right to see data we hold about their child.

- Requests must be made in writing.
- We will respond within one month.
- We may need to confirm your identity before sharing data.

We encourage families to regularly check and update the information we hold.

Sharing Data Without Consent

In serious cases, we may need to share data without consent – for example:

- Child protection concerns.
- Criminal investigations.
- Health and safety issues.
- Legal requirements.

Data Storage and Security

We keep data:

- In locked cabinets (paper files).
- In secure, password-protected systems (digital files).

Only authorised staff can access personal data.

To protect data, we:

- Keep IT systems updated.
- Use encryption for sensitive files.
- Shred paper files and permanently delete digital data when no longer needed.

Data Sharing

Internally: Shared only with staff who need it.

Externally: Shared when necessary, for example with:

- Local councils or other authorities.
- Emergency services.
- Approved service providers (e.g., IT support).

We never sell or share data for marketing.

Your Rights Under GDPR

You have the right to:

- See your data (access).
- Correct wrong information.
- Ask for data to be deleted (in some cases).
- Limit how your data is used.
- Move your data to another service.
- Object to certain types of data use.

Requests should be made in writing to the Board of Trustees.

Data Breaches

If a data breach happens:

- It will be reported to the Board of Trustees immediately.
- We will investigate and take action.

- If required, we will inform affected individuals and the ICO within 72 hours.

Roles and Responsibilities

Board of Trustees responsibilities:

- Make sure we follow data protection laws.
- Handle data protection concerns.
- Carry out regular reviews and audits.

Staff and volunteers must:

- Follow this policy.
- Report any concerns or breaches.
- Attend data protection training when needed.

Next Review Date: 31 August 2026