Policy

Al-Jamiatul Islamiyah
الجامعة الاسلامية
Institute of Higher Islamic Education

Data Protection Policy

Nurturing today's young people,
Inspiring tomorrow's exemplary citizens

Al-Jamiatul Islamiyah, Darul Uloom, Willows Lane, Bolton, Lancashire, BL3 4HF, UK.

Admin Office Tel: 01204 62622 – Email: info@boltondarululoom.org.uk – Website: www.boltondarululoom.org.uk

Document Control

Date of Last Review	**APRIL 2021**
Reviewed By	**Mr Irfan Ibrahim**
Approved by	**Chair of Governors'**
Review Period	**2 Years or as and when required**
Version	**2**
Date of Next Review	**APRIL 2023**

Contents

SECTION 1 – POLICY STATEMENT

AJI aims to ensure that all personal data collected about staff, pupils, parents, governors, trustees, visitors and other individuals are collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

This policy is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests. It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

SECTION 2 – TERMS USED WITHIN THIS POLICY

Personal Data	Any information relating to an identified, or identifiable, individual. This may include the individual's name (including initials), ID number, location data or online identifier, such as a username. 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: • Racial or ethnic origin. • Political opinions. • Religious or philosophical beliefs. • Trade union membership. • Genetics. • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes. • Health – physical or mental. • Sex life or sexual orientation.
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 Controller	A person or organisation that determines the purposes and the means of processing of personal data.
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.

SECTION 3 – THE DATA CONTROLLER

AJI processes personal data relating to parents, pupils, staff, trustees, visitors and others, and therefore is a data controller.

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

SECTION 4 – ROLES & RESPONSIBILITIES

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf.

The **Board of Trustees and Governors** has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

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

The **Data Protection Officer (DPO**) is responsible for:

- Overseeing the implementation of this policy.
- Developing policies and guidelines (inc. reviewing this policy every 2 years).
- Monitoring our compliance with data protection law.
- Training members of staff as part of the induction process.
- Providing CPD where changes to legislation, guidance or the school's processes make it necessary.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO. Our DPO is Mr Usman Mayat.

All staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy.
- Informing the school of any changes to their personal data, such as a change of address.
- Contacting the DPO if they have any questions, concerns or suggestions, and in the event of a data breach.

SECTION 5 – DATA PROTECTION PRINCIPLES

The Data Protection Act 2018 requires that personal data must be:

- Processed fairly, lawfully and transparently.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to only what is necessary to fulfil the purposes for which they are processed.
- Accurate and, where necessary, kept up to date.
- Kept for no longer than is necessary for the purposes for which they are processed.
- Processed in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

This policy sets out how we aim to comply with these principles.

SECTION 6 – LAWFUL BASES

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The individual (or their parent/guardian when appropriate in the case of a pupil) has freely given clear consent.
- The data needs to be processed so that the school can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering into a contract.
- The data needs to be processed so that the school can comply with a legal obligation.
- The data needs to be processed to ensure the vital interests of the individual, e.g. to protect someone's life.
- The data needs to be processed so that a public authority can perform a task in the public interest and carry out its official functions.
- The data needs to be processed for the legitimate interests of the school or a third party (provided the individual's rights and freedoms are not overridden).

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

SECTION 7 – LIMITATION, MINIMISATION AND ACCURACY

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's data retention policy.

SECTION 8 – SHARING PERSONAL DATA

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/guardian that puts the safety of our staff at risk.
- We need to liaise with other agencies – we will seek consent as necessary before doing this.
- 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 data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, 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, and information necessary to keep them safe while working with us.

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud.
- The apprehension or prosecution of offenders.
- The assessment or collection of tax owed to HMRC.
- In connection with legal proceedings.
- Where the disclosure is required to satisfy our safeguarding obligations.

- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

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.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

SECTION 9 – DATA SUBJECT RIGHTS

Data subjects have the following rights with regards to their personal information:

- The right to be informed about the collection and the use of their personal data.
- The right to access personal data and supplementary information.
- The right to have inaccurate personal data rectified, or completed if it is incomplete.
- The right to erasure (to be forgotten) in certain circumstances.
- The right to restrict processing in certain circumstances.
- The right to data portability, which allows the data subject to obtain and reuse their personal data for their own purposes across different services.
- The right to object to processing in certain circumstances.
- Rights in relation to automated decision making and profiling.
- The right to withdraw consent at any time (where relevant).
- The right to complain to the Information Commissioner.

SECTION 10 – SUBJECT ACCESS REQUESTS

SECTION 10.1 – SUBJECT ACCESS REQUESTS

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal 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 the data will be stored for, or if this isn't possible, the criteria used to determine this period.

- 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.

Subject access requests must be submitted in writing, either by letter or email to the DPO. They should include:

- 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.

SECTION 10.2 – CHILDREN AND SUBJECT ACCESS REQUESTS

Personal data about a child belongs to that child, and not the child's parents or guardians. For a parent or guardian to make a subject access request with respect to 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 aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or guardians 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.

SECTION 10.3 – RESPONDING ON SUBJECT ACCESS REQUESTS

When responding to requests, we:

- May ask the individual to provide 2 forms of identification.
- May contact the individual via phone to confirm the request was made.
- Will respond without delay and within 1 month of receipt of the request.
- Will provide the information free of charge.
- May tell the individual we will comply within 3 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 will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual.
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests.
- Is contained in adoption or parental order records.
- Is given to a court in proceedings concerning the child.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

SECTION 11 – OTHER DATA PROTECTION RIGHTS OF THE INDIVIDUAL

In addition to the right to make a subject access request, 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 processing at any time.
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances).
- Prevent use of their personal data for direct marketing.
- Challenge processing which has been justified on the basis of public interest.
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area.
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them).
- Prevent processing that is likely to cause damage or distress.
- Be notified of a data breach in certain circumstances.
- Make a complaint to the ICO.
- Ask for their personal 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.

SECTION 12 – PARENTAL REQUESTS TO SEE THE EDUCATIONAL RECORD

As we are an independent school, there is no automatic parental right of access to the educational record of your child. However, where a reasonable request is made, consideration will be given to provide this information judged on a case-by-case basis.

SECTION 13 – CCTV

We use CCTV in and around the school site for a variety of reasons as outlined in our CCTV Policy.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and prominent signs are placed at all main entrances explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the DPO.

Please see our CCTV Recording Policy for further details.

SECTION 14 – DATA SECURITY AND STORAGE OF RECORDS

We will protect personal data and keep it safe from unauthorised or unlawful 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, pinned to notice/display boards, or left anywhere else where there is general access.
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices.
- Staff, pupils or governors/trustees who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment *(See our E-Safety Policy).*

- 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.

SECTION 15 – DISPOSAL OF RECORDS

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date 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.

SECTION 16 – PERSONAL DATA BREACHES

The school will take all reasonable steps to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure outlined in **Appendix 1.**

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- Safeguarding information being made available to an unauthorised person.
- Non-anonymised pupil exam results or staff pay information being shared with trustees.
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked.
- The school's direct debit merchant being hacked and parents' financial details stolen.

SECTION 17 – LINKS WITH OTHER POLICIES

This policy is linked to our:

- *Data retention policies*
- *Privacy notices to parents, pupils and staff*
- *E-Safety Policy (inc. the Acceptable Use Agreement)*
- *CCTV Policy*

APPENDIX 1 – PERSONAL DATA BREACH PROCEDURE

1 On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO.

2 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.

3 The DPO will alert the Headteacher and the Chair of Governors.

4 The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.

5 The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.

6 The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis.

To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

- Loss of control over their data.
- Discrimination.
- Identify theft or fraud.
- Financial loss.
- Unauthorised reversal of pseudonymisation (for example, key-coding).
- Damage to reputation.
- Loss of confidentiality.
- Any other significant economic or social disadvantage to the individual(s) concerned.

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

7 The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach.

8 Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. 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.

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

10 The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

- 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.

11 The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.

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

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

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

ACTIONS TO MINIMISE THE IMPACT OF DATA BREACHES

We will take all necessary actions to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. **We will review the effectiveness of these actions and amend them as necessary after any data breach. For example, in case of:**

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 to recall it.
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.