MADNI TRUST

Jamia Al-Hudaa Nottingham

Data Protection Policy

Date: May 2018
Review Date: May 2019

To be reviewed by:
Data Protection Officer: Mohammed Amaar Sajjad

Contents

1. Introduction

On the 25th May 2018 the General Data Protection Regulation (GDPR) will be applicable and the current Data Protection Act (DPA) will be updated by a new Act giving effect to its provisions. Before that time the DPA will continue to apply.

This Policy sets out the manner in which personal data of staff, students and other individuals is processed fairly and lawfully.

Jamia Al-Hudaa collects and uses personal information about staff, students, parents or carers and other individuals who come into contact with the School. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the School complies with its statutory obligations.

Jamia Al-Hudaa is a data controller and must therefore comply with the Data Protection Principles in the processing of personal data, including the way in which the data is obtained, stored, used, disclosed and destroyed. The School must be able to demonstrate compliance. Failure to comply with the Principles exposes the School and staff to civil and criminal claims and possible financial penalties.

Details of the School's purpose for holding and processing data can be viewed on the Privacy notice of the school.

The Schools registration number is **Z5505235**.This registration is renewed annually and up dated as and when necessary.

2. Aim

This Policy will ensure:

- The School processes person data fairly and lawfully and in compliance with the Data Protection Principles.
- All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities under this policy.
- That the data protection rights of those involved with the School community are safeguarded.
- Confidence in the School's ability to process data fairly and securely.

3. Scope of policy

Jamia Al-Hudaa collects and uses personal information about staff, students, parents or carers and other individuals who come into contact with the Jamia. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the Jamia complies with its statutory obligations.

Jamia Al-Hudaa has a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website. Jamia also have a duty to issue a Fair Processing Notice to all students/parents or carers, this summarises the information held on students, why it is held and the other parties to whom it may be passed on.
This Policy applies to:

- Personal data of all School employees, governors, students, parents and carers, volunteers and any other person carrying out activities on behalf of the School.

- The processing of personal data, both in manual form and on computer.
- All staff and governors.

The Data Protection Principles

The School will ensure that personal data will be:

1. Processed fairly, lawfully and in a transparent manner.

2. Collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with those purposes.

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which data is processed.

4. Accurate and, where necessary, kept up to date.

5. Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

6. Processed in a way that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The School will be able to demonstrate compliance with these principles.

The School will have in place a process for dealing with the exercise of the following rights by Governors, staff, students, parents and members of the public in respect of their personal data:

- to be informed about what data is held, why it is being processed and who it is shared with;
- to access their data;
- to rectification of the record;
- to erasure;
- to restrict processing;
- to data portability;
- to object to processing;
- not to be subject to automated decision-making including
- profiling.

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

What is Personal or sensitive Information?

Personal data is information that relates to an identifiable living individual that is processed as data. Processing amounts to collecting, using, disclosing, retaining or disposing of information. The General Data Protection Regulation principles apply to all information held electronically or in structured paper files.

The principles also extend to educational records – the names of staff and children, dates of birth, addresses, national insurance numbers, school marks, medical information, SEN assessments and staff development reviews.

Sensitive personal data is information that relates to;

- race and ethnicity,
- political opinions,
- religious beliefs,
- membership of trade unions,
- physical and mental health,
- sexuality
- criminal offences

Sensitive personal data is given greater legal protection as individuals would expect certain information to be treated as private or confidential – for example, a pre-school manager may have a pre-school e-mail account that is made publicly available on the school's website whereas their home e-mail account is private and confidential and should only be available to those to whom consent had been granted.

4. Roles & Responsibilities

The Trustees and the Head Teacher are responsible for implementing good data protection practices and procedures within the School and for compliance with the Data Protection Principles.

It is the responsibility of all staff to ensure that their working practices comply with the Data Protection Principles. Disciplinary action may be taken against any employee who breaches any of the instructions or procedures forming part of this policy

A designated member of staff, the Data Protection Officer, will have responsibility for all issues relating to the processing of personal data and will report directly to the Trustees.

The Data Protection Officer will comply with responsibilities under the GDPR and will deal with subject access requests, requests for rectification and erasure, data security breaches. Complaints about data processing will be dealt with in accordance with the Schools Complaints Policy.

All staff are responsible for ensuring that personal data which they process is kept securely and is not disclosed to any unauthorised third parties.
Access to personal data should only be given to those who need access for the purpose of their duties. All staff will comply with the E-safety Policy.
Staff who work from home must have particular regard to the need to ensure compliance with this Policy and the E-safety Policy.
All staff will be aware of and follow the data breach security management process.

5. Data Security and Data Security Breach Management

Data protection breaches could be caused by a number of factors. A number of examples are shown below:

- Loss or theft of pupil, staff or governing body data and/ or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment Failure;
- Poor data destruction procedures;

- Human Error;
- Cyber-attack;
- Hacking.

In the event of a personal data breach, the Data Protection Officer should be notified immediately and an investigation carried out.

Appendix 1 is a template that can be used to report a breach.

See **Appendix 2** in relation to advice offered to staff at Jamia.

It is important to first evaluate the scale of any breach by considering the amount and nature of data and any immediate repercussions of a breach. In the case of a breach, the Senior Management will work with the Data Protection Officer to look at the following;

1- Containment & Recovery
2- Assessment of Risks
3- Consideration of further notification
4- Evaluation & Response

Appendix 3 offers an outline for staff to evaluate the seriousness of a breach and contact leads.

6. Subject Access Requests

Requests for access to personal data (Subject Access Requests)(SARs) will be processed by the Data Protection Officer. The Jamia may charge for the request to cover the costs of administration but in most cases there will be no charge. Records of all requests will be maintained.

The School will comply with the statutory time limits for effecting disclosure in response to a Subject Access Request. The statutory time limit of one calendar month (upon receipt of the request) applies from the 25th of May 2018.

Taking Action on a subject access request

1) Requests can be made in any way or form; verbal or written. It is not necessary for it to be addressed to the relevant department as long as the request is clearly linked to the subject's personal data.
2) The identity of the requestor must be established (as a legal obligation) before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child.

Evidence of identity can be established by requesting production of:

- Passport
- Driving Licence
- Utility bills with the current address
- Birth / Marriage certificate
- P45/P60
- Credit Card or Mortgage statement

This list is not exhaustive.

7. Complaints

Complaints will be dealt with in accordance with the Jamia Al-Hudaa's complaints policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

8. Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years. The policy review will be undertaken by the Data Protection Officer in consultation with the Senior Leadership Team.

9. Contacts

If you have any enquires in relation to this policy, please contact Mohammed Amaar Sajjad, Data Protection Officer, at admin@jamiaalhudaa.com or 0115 969 0800 who will also act as the contact point for any subject access requests.

Further advice and information is available from the information Commissioner's Office, www.ico.gov.uk or telephone 01625 5457453.

Appendix 1 Data Breach Reporting Form

Description of the Data Breach	
Time & Date breach was identified and by whom	
Who is reporting the breach: Name/Position/Department	
Contact Details: Telephone/Email	
Classification of Data breached: **i) Public Data** **ii) Internal Data** **iii) Confidential Data** **iv) Highly Confidential data**	
Volume of Data involved	
Confirmed or suspected breach	
Is the Breach contained or ongoing?	
If ongoing, what actions are being taken to recover the Data?	
Who has been informed of the Breach?	
Any Other Relevant Information?	
Email to admin@jamiaalhudaa.com or phone 0115 969 0800 to inform the Data Protection Officer that a form is being sent.	
Received By:	
Date/Time:	

Appendix 2 Advice for Staff

What staff should do:
DO get the permission of your manager to take any confidential information home.
DO transport information from school on secure computing devices (i.e. encrypted laptops and encrypted memory sticks). Wherever possible avoid taking paper documents out of the office.
DO use secure portable computing devices such as encrypted laptops and encrypted USB memory sticks when working remotely or from home.
DO ensure that any information on USB memory sticks is securely deleted off the device, or saved on a School shared drive.
DO ensure that all paper based information that is taken of premises is kept confidential and secure, ideally in a sealed envelope which indicates a return address if misplaced.
DO ensure that any confidential documents that are taken to your home are stored in a locked drawer.
DO ensure that paper based information and laptops are kept safe and close to hand when taken out off premises. Never leave them unattended. Particular care should be taken in public places (e.g. reading of documentation on public transport).
DO ensure that when transporting paper documentation in your car that it is placed in the boot (locked) during transit.
DO return the paper based information to the School as soon as possible and file or dispose of it securely.
DO report any loss of paper based information or portable computer devices to your line manager immediately.
DO ensure that all postal and e-mail addresses are checked to ensure safe dispatch of information.
DO ensure that when posting/emailing information that only the specific content required by the recipient is sent.
DO use pseudonyms and anonymise personal data where possible.
DO ensure that access to SIMS (or equivalent) is restricted to appropriate staff only, that leavers are removed in a timely manner and that any generic user names are disabled.

What staff must not do:
DO NOT take confidential information to an entertainment or public place such as a pub or cinema, whether held on paper or an electronic device. Any information must be taken to the destination directly and never left unattended during the journey.
DO NOT unnecessarily copy other parties into e-mail correspondence.
DO NOT e-mail documents to your own personal computer.
DO NOT store work related documents on your home computer.
DO NOT leave personal information unclaimed on any printer or fax machine.
DO NOT leave personal information on your desk overnight, or if you are away from your desk in meetings.
DO NOT leave documentation in vehicles overnight.
DO NOT discuss case level issues at social events or in public places.
DO NOT put confidential documents in non-confidential recycling bins.
DO NOT print off reports with personal data (e.g. pupil data) unless absolutely necessary.
DO NOT use unencrypted memory sticks or unencrypted laptop.

Appendix 3 Evaluating Criticality of a Breach

High Criticality: Major Incident	Contact:
• Highly Confidential/Confidential Data • Personal data breach involves >1000 individuals • External 3rd Party Data Involved • Significant or irreversible consequences • Likely Media Coverage • Immediate response required whether it is contained or not • Requires significant response beyond normal operating procedures	**Lead responsible Officer:** • To be determined via consultation of DPO with Trustees/SLT. **Other Possible Relevant Contacts:** • Internal Senior Managers • External Parties: Police, ICO, Individuals Impacted.
Moderate Criticality: Serious Incident	**Contact:**
• Confidential Data • Not contained within school • Personal data breach involves >100 individuals • Significant inconvenience will be experienced by individuals impacted • Incident may not yet be contained • Incident does not require immediate response • Incident response may require notification to Senior management team	**Lead responsible Officer:** • Data Protection officer (DPO) or head of school or department affected by incident. **Other Possible Relevant Contacts:** • Internal Senior Managers • Trustees • ICO, Police.
Low Criticality: Minor Incident	**Contact:**
• Internal or Confidential Data • Risk to school is low • Small number of individuals involved • Inconvenience may be experienced by individuals impacted • Loss of data is contained/encrypted • Incident can be responded to during working hours **Example:** Email sent to wrong recipient Loss of encrypted mobile device	**Lead responsible Officer:** • Data Protection officer (DPO) or head of school or department affected by incident. **Other Possible Relevant Contacts:** • Internal Senior Managers • Trustees