Lady Aisha Academy Data Protection Policy

Contents

Introduction

Lady Aisha Academy collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is necessary to process in order for the school to perform its official functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

Lady Aisha Academy intends to comply fully with the requirements and principles of the Data Protection Act 1998 prior to 25th May 2018, (as amended, undated or re-enacted from time to time) and from 25th May 2018, the (EU) 2016/679 Regulation of the European Parliament and of the Council of 27th April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (GDPR) and any national laws implementing the GDPR in the United Kingdom (all as amended, updated or re-enacted from time to time), and any applicable law or regulation which supersedes or replaces any of the foregoing in the United Kingdom.

Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 1998 and the 2016/679 General Data Protection Regulations. It is to provide transparency regarding whose data is held in the school, what is done with that data and who it is passed on to. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

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

Definitions

Personal information or data is defined as information relating to a natural identifiable person, whether directly or indirectly such as dates of birth and salaries.
Special category data is defined as highly sensitive pieces of information about people such as race, ethnicity, political opinions, religious beliefs and health.

Principles

In order to comply with the above mentioned regulations, Lady Aisha Academy upholds the following principles regarding personal and special category data, which is that:

1. All data is processed fairly and lawfully

2. All data is obtained for specified and lawful purposes and is processed under the following lawful bases: Consent, contract, legal obligation, vital interests, public tasks and / or legitimate interests.

3. Data obtained is adequate, relevant and not excessive

4. Data is accurate and where necessary, kept up to date

5. Data processed for any purpose is not kept for longer than the retention period, after which it is either transferred securely to the archives or destroyed appropriately. (For more detailed information, please see data retention policy)

6. Data subjects are informed of their data being processed during their child's registration (for students) and when signing their contracts (for employees). Data which requires consent (such as photographs and being contacted with fundraising/marketing material) is obtained on that day.

7. All data is kept secure and protected by an appropriate degree of security. Clear and robust safeguards are kept in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded

8. Data is not to be transferred to a country or territory outside the European Economic Area, without complying with the provisions of the Data Protection Legislation

9. Data is only shared with those agencies and organisations to whom there is a legal obligation to do so such as the Local Authority, DfE and social workers in safeguarding cases.

10. All information regarding the nature and processing of data is kept transparent through the following documents: the Data Ecosystem, the Data Asset Register, the Data Protection Impact Assessment and the Data Retention Policy. (These documents are available to view on the website and can alternatively be requested from the school office.)

Data subjects and their rights

The data subjects for Lady Aisha Academy are primarily the current pupils, parents of current pupils, current employees and visitors to the school. Data is also processed for job applicants, and children and their parents who have submitted application forms to the school for a place. Records are retained of pupils, their parents and staff who leave, for a required retention period after they have left. For further information and detail, please see the Data Retention Policy. (This is available to view on the website and can alternatively be requested from the school office).

Data subjects have the right to be informed of what data is held about them, thus during student registrations (for pupils and parents) and during signing staff contracts (for employees), data subjects will be informed of the data we retain and process about them, the avenues of communication we use with them, and their consent will be obtained for pictures to be taken and retained (for the newsletter / website / yearbook) and for their details to remain on our mailing list (to whom we send marketing and fundraising material). For a full, comprehensive list of exactly what data is stored and where, please see the Data Ecosystem. (This can be requested from the office).

All data which is collated and processed is necessary for the school to perform its official functions. Therefore, the other rights that data subjects usually have (the right to erasure, the right to restrict processing and the right to object) will not apply here. Regarding the right of access and the right to rectification, please see the section below on subject access requests. The rights in relation to automated decision making and profiling also do not apply at Lady Aisha Academy, as the school does not use any programmes or systems that make automated decisions.

Subject access requests

Data subjects have the right to access their data from the school and the right to rectify their data. This should be done through completing a subject access request, which essentially entails sending an email to the school at enquiries@ladyaisha.co.uk stating clearly what data you would like to access and title it Subject Access Request. Please be advised that you can only request data which applies to yourself and your child. Please see the Appendix for more information.

Other schools who also need to request information (such as UPNs, dates of birth, information relating to behaviour and on-rolling/off-rolling information) regarding a student who was previously at Lady Aisha Academy and is now attending their school should also send their requests via email. Information will not be given over the telephone.

Members of staff who need data that is not accessible to them should likewise email in their requests to the school office for what data they need (such as GCSE students' candidate numbers) and this will be emailed to them. Computerised data should not be written down or printed and given out. On those occasions when personal data is printed out and given to the teachers (such as risk assessments when going on trips), teachers should return the printed copies back to the office once they have finished with it, so that office staff can ensure that the printed information is securely destroyed / disposed of. Likewise, if teachers need to print data to the photocopier (such as pupils' assessment results for parent consultation meetings), they should alert the office beforehand so that office staff can remove the print-outs, and keep them in the office until the teacher can come to collect it. This will ensure that no students access the printed information.

Security of data

All data at Lady Aisha Academy is kept securely with restricted access. All computer accounts which are linked to the network are individually password protected. Not all data is accessible to staff accounts as some data is restricted only to administration and management accounts. All members of staff must ensure they log out of their accounts securely before they leave their computer, and must not allow any unauthorised person to use their account.

A firewall is set up for the school which mitigates outside attacks from the internet and the web filter Untangle is in place on all computers in the school. This is managed by AM Networking to whom we outsource all IT issues and who are also data processors for the school. There is a signed data sharing agreement in place between Lady Aisha Academy and AM Networking.

All data which is stored on Office 365 replicates and adds to the data on the school network. Again, only some data files are accessible to staff, with the rest restricted only to management and administration accounts. Documents on Office 365 are password protected and the data is also encrypted both at rest and transfer. All Office 365 users must log out of their accounts securely before they leave their computer, and must ensure that no unauthorised person uses their account.

Lady Aisha Academy shares its internet with the office at al-Madina Mosque, which is situated in the same complex. The data for Lady Aisha Academy is secure from them as they are not on the same network and therefore cannot access any of the school drives. The mosque office internet has very limited access to only a few people, and it is highly unlikely that an attack would originate from there. However, in the event that this should happen, this will be reported to the trustee of the mosque (Abdul Majeed) who will undertake a full investigation. In the event of a security breach taking place in the school, this will be reported to AM Networking (the school's data processors) Mr Aslam (the head teacher) and Nafeesa Mistry (the Data Protection Officer) who will carry out an internal investigation. In both cases the DPO will also inform the Information Commissioner's Office, the data subjects whose data has been breached (if appropriate) and this will be recorded in a breach log.

Al-Madina Mosque (who are the landlords of Lady Aisha Academy) uses CCTV cameras which are installed in the playground, in the sports hall and in the foyer entrance of the school. The CCTV is monitored by the mosque and not the school, but the school may request access to CCTV footage from the mosque if they wish to check up on anything.

All data that is recorded on paper is kept securely in lockable locations. This is comprised of three filing cabinets (two of which are in the office and one is upstairs between the staffroom and the head teacher's desk), a cupboard under the stairs and the exams cupboard in the office (which are constantly kept locked) and the office itself (which is always occupied by a member of staff and when left unattended, is locked.) For more details and information on where we store our data, please see the Data Ecosystem which can be requested from the office. For full information on data security and breaches, pleases see the Security and Breach section on the Data Asset Register, and for a full risk assessment on data kept in the school, please see the Data Protection Impact Assessment. (All of these documents can be requested from the school office.)

Data taken out of school by teachers

On certain occasions, such as when marking books and filling in assessment results and intervention strategies, teachers will take data home. In this case, teachers must ensure that students' information remains confidential and is not viewed by any other person. All data must be brought back to the school once it is no longer needed, and can only be kept at home for a suitable and appropriate purpose.

School meetings are carried out over Microsoft Teams, in the evenings at home. All participants of the meetings must ensure that nobody else can hear the meeting and that everything mentioned in the meeting is kept confidential.

On no account should any member of staff have pictures of pupils on their mobile phones. This is also emphasised upon in the staff code of conduct.

Complaints

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

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 DPO, head teacher, or nominated representative.

Contacts

If you have any enquires in relation to this policy, please contact the head teacher (Mr Aslam) or the Data Protection Officer (Nafeesa Mistry), 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 545745 ext. 3

Related documents and policies

- Data Retention Policy
- Data Protection Impact Assessment
- Data Asset Register
- Data Ecosystem (which includes the data map)
- E-Safety Policy

Appendix

Actioning a subject access request

1. Requests for information must be made in writing; which includes email, and be addressed to Mr Aslam or Nafeesa Mistry. If the initial request does not clearly identify the information required, then further enquiries will be made.

2. The identity of the requestor must be established 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.

3. Any individual has the right of access to information held about them. However, with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The head teacher or DPO should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

4. The school may make a charge for the provision of information, dependent upon the following:

- Should the information requested contain the educational record then the amount charged will be dependant upon the number of pages provided.
- Should the information requested be personal information that does not include any information contained within educational records, schools can charge up to £10 to provide it
- If the information requested is only the educational record viewing will be free, but a charge not exceeding the cost of copying the information can be made by the head teacher.

5. The response time for subject access requests, once officially received, is 40 days (not working or school days but calendar days, irrespective of school holiday periods). However, the 40 days will not commence until after receipt of fees or clarification of information sought

6. The Data Protection Act 1998 allows exemptions as to the provision of some information; therefore, all information will be reviewed prior to disclosure.

7. Third party information is that which has been provided by another, such as the police, Local Authority, health care professional or another school. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the 40-day statutory timescale.

8. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

9. If there are concerns over the disclosure of information then additional advice should be sought.

10. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

11. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

12. Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used, then registered/recorded mail must be used.

Reviewed by: N Mistry
September 2020

To be reviewed: September 2021