ASHTON WEST END PRIMARY ACADEMY

Academy Trust

William Street, Ashton-under-Lyne, Tameside, OL7 0BJ

DATA PROTECTION POLICY

Contents

Statement of intent

As an academy, we aim to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the its legal obligations under both and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill and the General Data Protection Regulation (GDPR).

The academy may, from time to time be required to share personal information about its staff or pupils with other organisation, including, but not limited to the Local Authority, The Department for Education and its associated agencies, the academy's payroll and Human Resources provider, other school and educational bodies and other outside agencies who may have a legitimate and vested interest.

Legislation

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It 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. In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

The Freedom of Information Act 2000, The Freedom of Information and Data Protection Regulations 2004.

Data Protection Principles

The GDPR is based on data protection principles that our academy must comply with.

The principles say that personal data must be:

• Processed lawfully, fairly and in a transparent manner

• Collected for specified, explicit and legitimate purposes

•Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed

• Accurate and, where necessary, kept up to date

• Kept for no longer than is necessary for the purposes for which it is processed

• Processed in a way that ensures appropriately security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

This policy sets out how the academy aims to comply with these principles.

Applicable Data

For the purpose of this policy, **personal data** is outlined as:

Any information relating to an identified, or identifiable, individual.
This may include the individual's:

- Name (including initials)
- Identification number
- Location data
- 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.

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

Accountability

The academy will endeavour to implement appropriate technical and organisational measure to demonstrate that data is processed in line with the principles as set out in the General data Protection Regulation (GDPR).

The academy will also provide comprehensive, clear and transparent privacy policy.

Records of activities relating to higher risk processing, including special categories of data or that in relation to criminal convictions and offences, including pending offences will be maintained.

Data Controller

Our Academy processes personal data relating to parents, pupils, staff, governors, visitors and others and therefore is a data controller. The academy is registered as a data controller with the Information commissioner's Office (ICO) and will renew this registration annually or as otherwise legally required.

Collecting personal data

The academy will ensure that the following are adhered to in the process of collecting and processing of data to include:

<u>Lawfulness, fairness and transparency</u>

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

- The data needs to be processed so that the academy can fulfil a contract with the individual, or the individual has asked the academy to take specific steps before entering into a contract
- The data needs to be processed so that the academy 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 the academy, as 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 academy or a third party (provided the individual’s rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent

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.
If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

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

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 will 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 Information and Records Management.

Consent

- Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes
- Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individuals wishes.
- Where consent is given, a record will be kept documenting how and when consent was given.
- The academy will ensure that consent will meet the standards as outlined in GDPR.

- Consent accepted under the Data Protection Act will be reviewed to ensure it meets the standards of GDPR
- Consent can be withdrawn by the individual at any time.
- The consent of parents will be sought prior to the processing of a child's data, except where the processing is related to preventative or counselling services offered directly to the child.

Subject access requests

Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the academy 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 Data Protection Officer (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.

Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer 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 below the age of 12 are generally not 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 carers of pupils at our academy may 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.

Responding to 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:

- May 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.

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.

Privacy by design

- We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:
- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge

- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

Personal data breaches

The term "personal data breach" refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

The Principal of the academy will ensure that all staff members are made aware of and understand what constitutes as a personal data breach.

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the ICO will be availed of the breach.

The academy's 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

All notifiable breaches will be reported to the ICO within 72 hours of the academy becoming aware of the breach.

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

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)

Records of all breaches will be stored on the academy's secure server.

The DPO and Principal (if different) will meet to review what happened and how it can be prevented in the future. This meeting will happen as soon as reasonably possible.

Data Security

The academy 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 will be kept securely.
- 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
- Secure passwords must be at least 8 characters long containing letters and numbers are to be used to access the academy's computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our policy on acceptable use)
- 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.

CCTV and photography

As part of our whole school activities, the academy may take photographs and record images of individuals within our school.
Written consent will be obtained from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

- On notice boards within the academy and in school magazines, brochures, newsletters, etc.
- Outside of the academy school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

Monitoring Arrangements

The academy's DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated and when necessary when legislation, in particular the Data Protection Act 2018 is amended. This policy will be reviewed every 2 years and shared with the full governing board.

DBS Data

All data provided by the Disclosure and Barring Service (DBS) will be handled in line with data protection legislation; this will include electronic communication.

Data provided by the DBs will never be duplicated

Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler