

# THE PREMIER ACADEMY



## **DATA PROTECTION POLICY**

### **Statement of Intent**

The Premier Academy is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under 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 organisations, mainly the LA, other schools and educational bodies, and potentially Children's Social Care Services.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the Academy complies with the following core principles of GDPR.

Organisational methods for keeping data secure are imperative, and the Academy believes that it is good practice to keep clear practical policies, backed up by written procedures.

### **Legal Framework**

This policy has due regard to legislation, including, but not limited to the following:

- The General Data Protection Regulation (GDPR)
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The Academy Standards and Framework Act 1998
- The Data Protection Act 2018

This policy will also have regard to the following guidance:

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'

This policy will be implemented in conjunction with the following Academy policies and documents:

- E-safety Policy
- Freedom of Information Policy
- Surveillance and CCTV Policy
- GDPR Privacy Notices
- Child Protection and Safeguarding Policy

### **Applicable Data**

For the purpose of this policy, personal data refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g. an

IP address. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data.

Sensitive personal data is referred to in the GDPR as 'special categories of personal data'. These specifically include the processing of genetic data, biometric data and data concerning health matters i.e. mental and physical health, nationality, ethnicity, and sexuality.

### **Principles**

In accordance with the requirements outlined in the GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be used in order to safeguard the rights and freedoms of individuals.
- Processed in a manner 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 GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

### **Accountability**

The Premier Academy will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

The Academy will provide clear privacy notices.

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

Internal records of processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

The Academy will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Data minimisation
- Transparency
- Allowing individuals to monitor processing
- Continuously creating and improving security features

Data protection impact assessments will be used, where appropriate.

### **Lawful Processing**

The legal basis for processing data will be identified and documented prior to data being processed.

The Academy will act as a data processor; however, this role may also be undertaken by other third parties.

Under the GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained

Processing is necessary for:

- Compliance with a legal obligation
- The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- Protecting the vital interests of a data subject or another person

Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent
- Processing relates to personal data manifestly made public by the data subject

Processing is necessary for:

- Carrying out obligations under employment, social security or social protection law, or a collective agreement
- Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
- The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
- Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)

### **Consent**

Consent will be sought prior to processing any data which cannot be done so under any other lawful basis, such as complying with a regulatory requirement.

Consent must be a positive indication. It cannot be inferred from silence, inactivity, 'opt-out' boxes or pre-ticked boxes.

Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

Where consent is given, a record will be kept documenting how and when consent was given. If verbal permission, via telephone or in person; the name of the parent/carer, date and time of permission will be recorded and passed on to the Atrium for record keeping. Only parents/carers stated on SIMS as a contact will be used for consent.

The Academy ensures that consent mechanisms meet the standards of the GDPR.

Consent accepted under the Data Protection Act will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

Consent can be withdrawn by the individual at any time.

Where a child is under the age of 16 the consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child.

### **Sharing Data Without Consent**

The Academy may share information without consent in specific circumstances. To determine whether information can be shared with consent, the Academy will identify one of the other lawful bases for processing:

**Contract** – the processing is necessary for a contract held between the Academy and individual, or because the individual has asked the Academy to take specific tests before entering into a contract.

**Legal Obligation** – the processing is necessary for the Academy to comply with the law (not including contractual obligations).

**Vital Interests** – the processing is necessary to protect someone’s life.

**Public Task** – the processing is necessary for the Academy to perform a task in the public interest or for its official functions, and the task or function has a clear basis in law.

**Legitimate Interests** – the processing is necessary for the Academy’s legitimate interests or the legitimate interests of a third party, unless there is good reason to protect the individual’s personal data, which overrides those legitimate interests.

Where the Academy is able to justify one of the lawful bases outlined above an exemption applies, or there is a requirement under another law, information may be shared without consent.

Specifically, the GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe, and information may be shared without consent if to gain consent would place a child at risk.

### **The Right To Be Informed**

The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The contact details of the controller (the Academy), and where applicable, the controller’s representative.
- The purpose of, and the legal basis for processing the data.
- The legitimate interests of the controller or third party.
- Any recipient or categories of recipients of the personal data.
- The retention period of criteria used to determine the retention period varies due to the nature of the data stored e.g. an incident which happens on a school visit needs to be kept until the child is 25 years of age.

The existence of the data subject’s rights, including the right to:

- Withdraw consent at any time
- Lodge a complaint with a supervisory authority

The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided.

Where data is not obtained directly from the data subject, information regarding the categories of personal data that the Academy holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.

For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

In relation to data that is not obtained directly from the data subject, this information will be supplied:

- Within one month of having obtained the data.
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
- If the data are used to communicate with the individual, at the latest, when the first communication takes place.

### **The Right Of Access**

Individuals have the right to obtain confirmation that their data is being processed.

Individuals have the right to submit a Subject Access Request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

The Academy will verify the identity of the person making the request before any information is supplied.

A copy of the information will be supplied to the individual free of charge; however, the Academy may impose a 'reasonable fee' to comply with requests for further copies of the same information.

Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

All fees will be based on the administrative cost of providing the information.

All requests will be responded to without delay and at the latest, within one month of receipt, if a request has been made for educational information then the request will be responded to within 15 school-days.

In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

Where a request is manifestly unfounded or excessive, the Academy holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

In the event that a large quantity of information is being processed about an individual, the Academy will ask the individual to specify the information the request is in relation to.

### **The Right To Rectification**

Individuals are entitled to have any inaccurate or incomplete personal data rectified.

Where the personal data in question has been disclosed to third parties, the Academy will inform them of the rectification where possible.

Where appropriate, the Academy will inform the individual about the third parties that the data has been disclosed to.

Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

Where no action is being taken in response to a request for rectification, the Academy will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

### **The Right To Erasure**

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected / processed.
- When the individual withdraws their consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed.
- The personal data is required to be erased in order to comply with a legal obligation.

The Academy has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information.
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- For public health purposes in the public interest.
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes.
- The exercise or defence of legal claims.

Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

Where personal data has been made public within an online environment, the Academy will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

### **The Right To Restrict Processing**

Individuals have the right to block or suppress the Academy's processing of personal data.

In the event that processing is restricted, the Academy will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

The Academy will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the Academy has verified the accuracy of the data.
- Where an individual has objected to the processing and the Academy is considering whether their legitimate grounds override those of the individual.
- Where processing is unlawful and the individual opposes erasure and requests restriction instead.
- Where the Academy no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.

If the personal data in question has been disclosed to third parties, the Academy will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

The Academy will inform individuals when a restriction on processing has been lifted.

### **The Right To Data Portability**

Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller.
- Where the processing is based on the individual's consent or for the performance of a contract.
- When processing is carried out by automated means.

Personal data will be provided in a structured, commonly used and machine-readable form.

The Academy will provide the information free of charge.

Where feasible, data will be transmitted directly to another organisation at the request of the individual.

The Academy is not required to adopt or maintain processing systems which are technically compatible with other organisations.

In the event that the personal data concerns more than one individual, the Academy will consider whether providing the information would prejudice the rights of any other individual.

The Academy will respond to any requests for portability within one month.

Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

Where no action is being taken in response to a request, the Academy will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

### **The Right To Object**

The Academy will inform individuals of their right to object at the first point of communication and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest.
- Direct marketing.
- Processing for purposes of scientific or historical research and statistics.

Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.
- The Academy will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the Academy can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the Academy is not required to comply with an objection to the processing of the data.

Where the processing activity is outlined above, but is carried out online, the Academy will offer a method for individuals to object online.

### **Automated Decision Making and Profiling**

Individuals have the right not to be subject to a decision when:

- It is based on automated processing, e.g. profiling.
- It produces a legal effect or a similarly significant effect on the individual.

The Academy will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

When automatically processing personal data for profiling purposes, the Academy will ensure that the appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.
- Using appropriate mathematical or statistical procedures.
- Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

Automated decisions must not concern a child or be based on the processing of sensitive data, unless:

- The Academy has the explicit consent of the individual.
- The processing is necessary for reasons of substantial public interest on the basis of Union/Member State law.

### **Privacy by Design and Privacy Impact Assessments**

The Academy will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the Academy has considered and integrated data protection into processing activities.

Data Protection Impact Assessments (DPIAs) will be used to identify the most effective method of complying with the Academy's data protection obligations and meeting individuals' expectations of privacy.

DPIAs will allow the Academy to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the Academy's reputation which might otherwise occur.

A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

A DPIA will be used for more than one project, where necessary.

High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling.

- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences.
- The use of CCTV and audio recording.

The Academy will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes.
- An assessment of the necessity and proportionality of the processing in relation to the purpose.
- An outline of the risks to individuals.
- The measures implemented in order to address risk.

Where a DPIA indicates high risk data processing, the Academy will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

### **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 Governing Body will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

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

The risk of the breach having a detrimental effect on the individual, and the need to notify the ICO, will be assessed on a case-by-case basis.

In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the Academy will notify those concerned directly.

A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the ICO.

In the event that a breach is sufficiently serious, the public will be notified without undue delay.

Effective and robust breach detection, investigation and internal reporting procedures are in place at the Academy, which facilitate decision-making in relation to whether the ICO or public need to be notified.

Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned.
- An explanation of the likely consequences of the personal data breach.
- A description of the proposed measures to be taken to deal with the personal data breach.
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects.

## **Data Security**

Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

Confidential paper records will not be left unattended or in clear view anywhere with general access.

Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.

Memory sticks must be password-protected.

All electronic devices are password-protected to protect the information on the device in case of theft.

Where possible, the Academy enables electronic devices to allow the remote blocking or deletion of data in case of theft.

All necessary members of staff are provided with their own secure login and password.

Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.

Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the Academy premises accepts full responsibility for the security of the data.

Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.

Under no circumstances are volunteers / visitors allowed access to confidential or personal information. Visitors to areas of the Academy containing sensitive information are supervised at all times.

The physical security of the Academy's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism / burglary / theft is identified, extra measures to secure data storage will be put in place.

The Academy takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

## **Publication of Information**

The Academy will not publish any personal data, including photos, on its website without parental consent.

When uploading information to the Academy website, staff are mindful of any metadata or deletions which could be accessed in documents and images on the site.

## **CCTV and Photography**

The Academy understands that recording images of identifiable individuals constitutes as processing personal data, so it is done in line with data protection principles.

The Academy notifies all children, staff and visitors of the purpose for collecting CCTV images via the privacy notice.

Cameras are only placed where they do not intrude on anyone's privacy and/or are necessary to fulfil their purpose for protection.

All CCTV footage will be kept for 30 days for security purposes; the Governing Body is responsible for keeping the records secure and allowing access.

The Academy will always indicate its intentions for taking photographs of children and will retrieve permission before publishing them.

If the Academy wishes to use images / video footage of children in a publication, such as the Academy website, prospectus, or recordings of Academy plays, written permission will be sought for the particular usage from the parent of the child.

Precautions, as outlined in the Surveillance and CCTV Policy and E-safety Policy, are taken when publishing photographs of children, in print, video or on the Academy website.

Images captured by individuals for recreational / personal purposes, and videos made by parents for family use, are exempt from the GDPR.

## **Data Retention**

Data will not be kept for longer than is necessary.

Unrequired data will be deleted as soon as practicable.

Personal data on a child is transferred to a new school on registration; where a child is missing in education the personal data is kept for a minimum of 10 years.

Some educational records relating to former children or employees of the Academy may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

**DBS Data**

All data provided by the DBS will be handled in line with data protection legislation; this includes 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.

**Policy Review**

This policy is reviewed every 2 years by the Governing Body. The next scheduled review date for this policy is March 2020.

**September 2018**