THE PREMIER ACADEMY

DATA PROTECTION POLICY – MARCH 2026

Statement of Intent

The Premier Academy is required to keep and process certain information about its staff members, parents/carers and children in accordance with its legal obligations under data protection legislation.

The Academy may, from time to time, be required to share personal information about its staff or children 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 core principles of the UK 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 all relevant legislation and statutory guidance including, but not limited to, the following:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018 (DPA 2018)
- The Data (Use and Access) Act 2025 (DUAA)
- The Education (Pupil Information) (England) Regulations 2005 (as amended)
- DfE 'Keeping Children Safe in Education'
- DfE (2026) 'Generative AI: Product Safety Standards

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

- Online Safety Policy
- Freedom of Information Policy
- Surveillance and CCTV Policy
- UK GDPR Privacy Notices
- Records Management Policy
- Child Protection 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 UK 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 UK GDPR as 'special categories of personal data'. These specifically include the processing of genetic data, biometric data (e.g. facial recognition or fingerprinting) and data concerning health matters, e.g. mental and physical health, nationality, ethnicity, and sexuality. Sensitive personal data does not include data about criminal allegations, proceedings or convictions.

In the case of criminal offence data, schools are only able to process this if it is either under the control of official authority or authorised by domestic law. The latter point can only be used if the processing is necessary for the purposes of performing or exercising obligations or rights imposed by law in connection with employment, social security, social protection, health or research.

Principles
In accordance with the requirements outlined in the UK 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 UK GDPR also requires that “the controller shall be responsible for, and able to demonstrate, compliance with the principles”.

Recognised Legitimate Interests

Under the Data (Use and Access) Act 2025, the Academy identifies certain processing activities as "Recognised Legitimate Interests." For these activities, the Academy is not required to perform a formal balancing test (Legitimate Interest Assessment), as the processing is deemed essential for the public good. These include:

- Safeguarding: Processing necessary for the purposes of safeguarding children or individuals at risk.
- Emergency Response: Processing necessary for responding to an emergency or ensuring public safety.
- Crime Prevention: Processing necessary for the detection or prevention of crime.

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 UK GDPR and DPA and will provide clear and transparent privacy policies. The Academy will also provide evidence that it is complying with UK GDPR and DPA.

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 also document other aspects of compliance with the UK GDPR and DPA where this is deemed appropriate in certain circumstances, including the following:
- Information required for privacy notices, e.g. the lawful basis for the processing
- Records of consent
- Controller-processor contracts
- The location of personal data
- Data Protection Impact Assessment (DPIA) reports
- Records of personal data breaches

The Academy will implement measures that meet the principles of data protection by design and data protection by default, such as:
- Minimising the processing of personal data
- Pseudonymising personal data as soon as possible
- Ensuring transparency in respect of the functions and processing of personal data
- Allowing individuals to monitor processing
- Continuously creating and improving security features

DPIAs will be used to identify and reduce data protection risks, where appropriate.

Data Protection Officer (DPO)

The Academy's appointed Data Protection Officer is the central point of contact for matters relating to data protection. The DPO works in conjunction with IT Partnership and Crescita HR on matters relating to data protection.

The DPO is appointed to:
- Inform and advise the Academy about their obligations to comply with the UK GDPR and other data protection laws.
- Monitor the Academy's compliance with the UK GDPR and other laws, including managing internal data protection activities, advising on DPIAs, conducting internal audits and providing the required training to staff members.
- Cooperate with the Commission (ICO) and act as the first point of contact for the Commission and for individuals whose data is being processed.

The DPO is responsible for:
- Coordinating a proactive and preventative approach to data protection.
- Calculating and evaluating the risks associated with the Academy's data processing.
- Having regard to the nature, scope, context and purposes of all data processing.
- Prioritising and focussing on more risky activities, e.g. where special category data is being processed.
- Promoting a culture of privacy awareness throughout the school community.
- Carrying out ad hoc reviews of data practices to ensure staff understand and are acting in accordance with relevant data protection laws.

- Providing annual training for all staff on the risks, limitations and lawful processing requirements when using generative artificial intelligence (AI) technologies.

The DPO will have professional experience and be highly knowledgeable about data protection law, particularly that in relation to schools. An existing employee will be appointed to the role of DPO provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests.

The DPO will operate independently and will not be dismissed or penalised for performing their duties. Sufficient resources and appropriate access will be provided to the DPO to enable them to meet their UK GDPR obligations.

The DPO will report to the highest level of management at the Academy, which is the Governing Body.

Staff will ensure that they involve the DPO in all data protection matters closely and in a timely manner.

Lawful Processing

The legal basis for processing data will be identified and documented prior to data being processed. Under the UK GDP, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained
- Processing is necessary for a contract held with the individual or because they have asked the Academy to take specific steps before entering into a contract
- Processing is necessary for compliance with a legal obligation (not including contractual obligations)
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- Processing is necessary for protecting vital interests of a data subject or another person, e.g. to protect someone's life
- Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject – this condition is not available to processing undertaken by the school in the performance of its tasks

The Academy will only process personal data without consent where any of the above purposes cannot reasonably be achieved by other, less intrusive means or by processing less data.

Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject
- 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
- Reasons of substantial public interest with a basis in law which is proportionate to the aim pursued and which contains appropriate safeguards
- The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services with a basis in law
- Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
- Archiving purposes in the public interest or scientific and historical research purposes or statistical purposes in accordance with a basis in law

When none of the above apply, consent will be obtained by the data subject to the processing of their special category personal data.

The Academy will ensure that it has privacy notices established which clearly outline the reasons why it needs to collect personal data. The privacy notice will include the following details:

- Why the Academy needs to collect personal data
- What the Academy plans to do with the personal data
- How long the Academy will keep the personal data
- Whether the Academy will share the personal data with any external organisations

The privacy notice will be clear and accessible to data subjects. The privacy notice will also be reviewed by the Academy at least annually and whenever significant changes are made to how the Academy processes the data that it collects.

The Academy will ensure that any parents/carers, children and staff whose personal data is included will be notified of any significant changes to the privacy notice or the way in which the Academy processes the data.

For personal data to be processed fairly, data subjects must be made aware:

- That the personal data is being processed.
- Why the personal data is being processed.
- What the lawful basis is for that processing.
- Whether the personal data will be shared and if so, with whom.
- The existence of the data subject's rights in relation to the processing of that personal data.
- The right of the data subject to raise a complaint with the Commission in relation to any processing.

The Academy has privacy notices for the following groups, which outline the information above that is specific to them:

- Prospective employees
- Pupils and their families
- School workforce
- Third parties
- Trustees and governors
- Volunteers

There may be circumstances where it is considered necessary to process personal data or special category personal data to protect the vital interests of a data subject. This may include medical emergencies where it is not possible for the data subject to give consent to the processing. In such circumstances, the Academy will make a decision only after seeking further clarification.

Consent

Consent must be a positive indication expressly confirmed. It cannot be inferred from silence, inactivity, a positive action without words 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. Consent can be withdrawn by the individual at any time.

Where consent is given, a record will be kept documenting how and when consent was given and what the data subject was told.

The Academy ensures that consent mechanisms meet the standards of the UK GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found or the processing must cease. Consent accepted under the DPA will be reviewed to ensure it meets the standards of the UK GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

When children and staff join the Academy, the staff member or child's parent/carer will be required to complete a consent form for personal data use. This consent form deals with the taking and use of photographs and videos, amongst other things. Where appropriate, third parties may also be required to compete a consent form.

The Right To Be Informed

Adults and children have the same right to be informed about how the Academy uses their data. The privacy notices supplied to individuals, including children, in regard to the processing of their personal data will be written in clear, plain, age-appropriate 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 identity and contact details of the controller, the controller's representative, where applicable and the DPO
- The purpose of and the lawful basis for, processing the data
- The legitimate interests of the controller or third party
- Any recipient or categories of recipients of the personal data
- Details of transfers to third countries and the safeguards in place
- The retention period of criteria used to determine the retention period
- 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 – this information will be supplied at the time the data is obtained.

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 – 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 and the right to submit a Subject Access Request (SAR) to gain access to their personal data 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 request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

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

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.

The Academy will ensure that information released in response to a SAR does not disclose personal data of another individual. If responding to the SAR in the usual way would disclose such data, the Academy will:

- Omit certain elements from the response if another individual's personal data would be disclosed otherwise.
- Reject requests that cannot be fulfilled without disclosing another individual's personal data, unless those individual consents or it is reasonable to comply without consent.
- Explain to the individual who made the SAR why their request could not be responded to in full.

If 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.

<u>Reasonable and Proportionate Searches</u>
When responding to a SAR, the Academy will carry out searches for personal data that are reasonable and proportionate. In determining what is proportionate, the Academy will consider the volume of data, the effort required to retrieve it and the complexity of the request. The Academy is not required to conduct an 'exhaustive' search where the administrative burden would be vastly disproportionate to the benefit to the requester, as determined by the DPO.

<u>"Stop the Clock" Provision</u>
The Academy may pause (stop the clock) the one-month response period in the following circumstances:

- Clarification: Where the Academy reasonably requires further information from the requester to locate the specific data requested.
- Identity Verification: Where the Academy requires evidence to verify the identity of the requester.

The response period will resume once the required information or verification is received. The requester will be notified immediately if the clock is paused.

The Right To Rectification

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

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

Requests for rectification will be investigated and resolved, where appropriate, free of charge; however, the Academy may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual makes multiple requests at once. The Academy reserves the right to refuse to process requests for rectification if they are manifestly unfounded or excessive or if exemptions apply.

The Academy will take reasonable steps to ensure that data is accurate or is rectified if inaccurate, implementing a proportional response for data that has a significant impact on the individual, e.g. if significant decisions are made using that data. The Academy will restrict processing of the data in question whilst its accuracy is being verified, where possible.

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.

Where no action is being taken in response to a request for rectification, or where the request has been investigated and the data has been found to be accurate, 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 personal data is processed in relation to the offer of information society services to a child

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.

If 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

The Academy will only ever conduct solely automated decision making with legal or similarly significant effects if the decision is:

- Necessary for entering into or performance of a contract.
- Authorised by law.
- Based on the individual's explicit consent.

Automated decisions will not concern a child nor use special category personal data, unless:

- The Academy has the explicit consent of the individual.
- The processing is necessary for reasons of substantial public interest.

The Academy will conduct a DPIA for automated decision making to mitigate risk of errors, bias and discrimination.

The Academy will ensure that individuals concerned are given specific information about the processing and an opportunity to challenge or request a review of the decision.

Generative AI systems will not be used to make solely automated decisions with significant effects on individuals, such as decisions regarding academic grading, behaviour sanctions, admissions, or staff appraisals, unless a suitably qualified person reviews and authorises the decision-making outcome.

Individuals have the right not to be subject to a decision when both of the following conditions are met:

- 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.

Data Protection by Design and Default

The Academy will act in accordance with the UK GDPR by adopting a data protection by design and default approach and implementing technical and organisational measures which demonstrate how the Academy has considered and integrated data protection into all aspects of processing activities. In line with the data protection by default approach, the Academy will ensure that only data that is necessary to achieve its specific purpose will be processed.

The Academy will implement a data protection by design and default approach by using a number of methods, including, but not limited to:

- Considering data protection issues as part of the design and implementation of systems, services and practices.

- Making data protection an essential component of the core functionality of processing systems and services.
- Automatically protecting personal data in school ICT systems.
- Implementing basic technical measures within the school network and ICT systems to ensure data is kept secure.
- Promoting the identity of the DPO as a point of contact.
- Ensuring that documents are written in plain language so individuals can easily understand what is being done with personal data.

Data Protection Impact Assessments (DPIAs)

DPIAs will be used in certain circumstances to identify the most effective method of complying with the Academy's data protection obligations and meeting individuals' expectations of privacy.

DPIAs will be conducted prior to the implementation of any generative AI tools where the processing of personal data is involved.

A DPIA will include specific evaluation of the risks associated with AI systems, including fairness, accuracy, accountability, transparency and security, in accordance with the DfE's 'Generative artificial intelligence in education (2025)' guidance.

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 and 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

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 Commission to seek its opinion as to whether the processing operation complies with the UK 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 training.

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 Commission or public need to be notified.

Where the Academy faces a data security incident, the DPO will coordinate an effort to establish whether a personal data breach has occurred, assess the significance of any breach and take prompt and appropriate steps to address it.

All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the Academy becoming aware of it. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed and the individuals concerned will be contacted directly. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority. The risk of the breach having a detrimental effect on the individual and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis. In the event that a breach is sufficiently serious, the public will be notified without undue delay.

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

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- 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

Where notifying an individual about a breach to their personal data, the Academy will provide specific and clear advice to individuals on the steps they can take to protect themselves and their data, where possible and appropriate to do so.

The Academy will ensure all facts regarding the breach, the effects of the breach and any decision-making processes and actions taken are documented in line with the UK GDPR accountability principle and in accordance with the Records Management Policy.

Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

The Academy will work to identify the cause of the breach and assess how a recurrence can be prevented, e.g. by mandating data protection refresher training where the breach was a result of human error.

Data Security

Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access and 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/carers are sent via 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 UK GDPR seriously and any unauthorised disclosure may result in disciplinary action.

When disposing of data, paper documents will be shredded and digital storage devices will be physically destroyed when they are no longer required. ICT assets will be disposed of in accordance with the Commission's guidance on the disposal of ICT assets.

The Academy holds the right to take the necessary disciplinary action against a staff member if they believe them to be in breach of the above security measures.

Safeguarding

Data protection law is not a barrier to sharing information where there are concerns about the welfare or safety of a child. The Academy will always prioritise the best interests of the child. Staff are empowered to share relevant information with authorities and partners where it is necessary to protect a child from harm, relying on the 'Recognised Legitimate Interest' of safeguarding.

The Academy will aim to gain consent to share information where appropriate; however, will not endeavour to gain consent if to do so would place a child at risk. The Academy will manage all instances of data sharing for the purposes of keeping a child safe in line with the Child Protection Policy.

Children's personal data will not be provided where the serious harm test is met. Where there is doubt, the Academy will seek independent legal advice.

Publication of Information

The Academy publishes a Freedom of Information Publication Scheme on its website outlining classes of information that will be made routinely available, including:
- Policies and procedures.
- Minutes of meetings.

- Annual reports.
- Financial information.

Classes of information specified in the Freedom of Information Publication Scheme are made available quickly and easily on request.

The Academy will not publish any personal information, including photos, on its website without the permission of the affected individual. When uploading information to the Academy website, staff are considerate 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 3 months 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, permission will be sought for the particular usage from the parent/carer of the child.

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

Parents/carers and others attending Academy events are able to take photographs and videos of those events as long as they are for domestic purposes only. Photographs or videos being used for any other purpose are prohibited to be taken by parents/carers or visitors to the Academy.

The Academy asks that parents/carers and others do not post any images or videos which include any child other than their own child(ren) on any social media or otherwise publish those images or videos.

Cloud Computing

For the purposes of this Policy, 'cloud computing' refers to storing and accessing data and programs, such as documents, photos or videos, over the internet, rather than on a device's hard drive. Cloud computing involves the Academy accessing a shared pool of ICT services remotely via a private network or the internet.

All staff will be made aware of data protection requirements and how these are impacted by the storing of data in the cloud, including that cloud usage does not prevent data subjects from exercising their data protection rights.

If the cloud service offers an authentication process, each user will have their own account. When assessing any cloud-based or AI-powered service, the Academy will ensure that the provider

demonstrates UK GDPR compliance, provides explicit guarantees regarding non-retention of input data and allows the Academy to audit or verify compliance where necessary. The use of any cloud services which involve AI processing will be subject to a prior risk assessment and will require a DPIA where personal data is involved. A system will be implemented to allow user accounts to be created, updated, suspended and deleted and for credentials to be reset if they are forgotten, lost or stolen. Access for employees will be removed when they leave employment of the Academy.

All files and personal data will be encrypted before they leave an academy device and are placed in the cloud, including when the data is 'in transit' between the device and cloud. A robust encryption key management arrangement will be put in place to maintain protection of the encrypted data. The loss of an encryption key will be reported to the DPO immediately; failure to do so could result in accidental access or destruction of personal data and, therefore, a breach of the relevant data protection legislation.

As with files on school devices, only authorised parties will be able to access files on the cloud. An audit process will be put in place to alert the Academy should unauthorised access, deletion or modification occur and ensure ongoing compliance with the school's policies for the use of cloud computing.

The Academy's usage of cloud computing, including the service's security and efficiency, will be assessed and monitored by the DPO and IT Partnership. They will also ensure that a contract and data processing agreement are in place with the service provider, confirming compliance with the principles of the UK GDPR and DPA. The agreement will specify the circumstances in which the service provider may access the personal data it processes, such as the provision of support services.

The Academy will also:

- Ensure that the service provider has completed a comprehensive and effective self-certification checklist covering data protection in the cloud.
- Ensure that the service provider can delete all copies of personal data within a timescale in line with the Academy's Data Protection Policy.
- Confirm that the service provider will remove all copies of data, including back-ups, if requested.
- Find out what will happen to personal data should the Academy decide to withdraw from the cloud service in the future.
- Assess the level of risk regarding network connectivity and make an informed decision as to whether the Academy is prepared to accept that risk.
- Monitor the use of the cloud service, with any suspicious or inappropriate behaviour of children, staff or parents/carers being reported directly to the CEO.

Generative Artificial Intelligence (AI)

The Academy is committed to the safe and transparent use of AI in education, in line with DfE (2026) Safety Standards.

- Data Protection Impact Assessments (DPIA): A DPIA must be completed before any AI tool is introduced that processes personal data.
- Training Prohibitions: The Academy will not use AI products that utilise child or staff work (including intellectual property) to train or fine-tune commercial models without explicit, informed consent.
- Human Oversight: No solely automated decision-making (ADM) will be used for high-stakes decisions (e.g. admissions, exclusions or SEND assessments). All AI-generated outputs must

be reviewed by a member of staff. The Academy accepts no liability for decisions made solely on unverified AI outputs.
- Safeguarding Flags: AI tools used by children must include robust filtering and monitoring. If an AI tool detects signs of distress or safeguarding risks, it must automatically flag this to the Designated Safeguarding Lead (DSL).

Data Protection Complaints

Individuals have the right to complain if they believe the Academy has mishandled their personal data.
- Complaints should be made in the first instance to the Academy.
- The Academy will acknowledge receipt of a complaint within 30 days. We aim to provide a full response and resolution without undue delay.
- Requesters must engage with the Academy's internal complaints process before escalating a matter to the Commission.

Data Retention

Data will not be kept for longer than is necessary. Unrequired data will be deleted as soon as practicable. 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.

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.

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 annually by the Governing Body.