Policy and procedure for

Data Protection

Reviewed by CEO: Autumn 2026

Please note: The Data (Use and Access) Act 2025 (DUAA) amends, but does not replace, the UK GDPR, DPA and Privacy and Electronic Communications Regulations. References in this policy to those laws include them as amended by the DUAA.

Contents

1. Legal framework 0
2. Applicable data 0
3. Accountability 2
4. Data protection officer (DPO) 3
5. Lawful processing 4
6. Consent 7
7. The right to be informed 7
8. The right of access 8
9. The right to rectification 10
10. The right to erasure 10
11. The right to restrict processing 11
12. The right to data portability 12
13. The right to object 13
14. Informing data subjects 14
15. Information rights requests 14
16. Data protection complaints 15
17. Automated decision making and profiling 16
18. Data protection by design and default 17
19. Data Protection Impact Assessments (DPIAs) 18
20. Data breaches 18
21. Data security 19
22. Safeguarding 21
23. Publication of information 22
24. CCTV and photography 22
25. Procurement and management of educational technology 23
26. Cloud computing 25
27. Use of generative artificial intelligence (AI) 26
28. Data retention 27
29. DBS data 27
30. Monitoring and review 27

Annex A - AET Subject Access Request Procedure 28

Annex B - AET Data breach internal procedure to follow 29

Statement of intent

All AET policies are written to support our schools and communities. We do this by ensuring they are always in line with our Colleague Values:



Applying these values to everything we do means always acting with integrity, in the interests of others, being honest, open and transparent and putting the safety of our children first.

The Aspire Educational Trust is required to keep and process certain information about its staff members, pupils, their families, volunteers and external contractors in accordance with its legal obligations under data protection legislation.

The trust and its schools may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the DfE, LA, other schools and educational bodies, and potentially children's services.

This policy is in place to ensure all staff, local academy committee governors and trustees are aware of their responsibilities and outlines how the trust complies with the following core principles of the UK GDPR.

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

1. 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)
- Data Protection Act 2018 (DPA)
- School Standards and Framework Act 1998
- Freedom of Information Act 2000
- Data (Use and Access) Act 2025 (DUAA)
- Electronic Commerce (EC Directive) Regulations 2002
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2018)
- Protection of Freedoms Act 2012
- DfE 'Keeping children safe in education'

This policy also has regard to the following guidance:

- ICO 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- DfE ' Data protection in schools'
- DfE ' The Data Use and Access Act 2025'
- ICO 'Data (Use and Access) Act 2025' guidance
- DfE Generative artificial intelligence (AI) in education
- DfE ' Generative AI: product safety standards'

This policy operates in conjunction with the following trust or school policies:

- Photography and Images Policy
- Cyber-security Policy
- Freedom of Information Policy
- Freedom of Information Publication Scheme
- Surveillance and CCTV Policy
- Child Protection and Safeguarding Policy
- Records Management Policy

2. 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 and pseudonymised data, e.g. key-coded.

'Sensitive personal data' is referred to in the UK GDPR as 'special categories of personal data', and is defined as:

- Genetic data.
- Biometric data.
- Data concerning health.
- Data concerning a person's sex life.
- Data concerning a person's sexual orientation.
- Personal data which reveals:
  - Racial or ethnic origin.
  - Political opinions.
  - Religious or philosophical beliefs.
  - Trade union membership.
  - Principles.

'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 conditions of the reason for storing and requiring the data fall into one of the conditions below:

- The processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller of the data subject in connection with employment, social security, social protection, health or social care purposes, public health, and research.

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 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 processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the UK GDPR 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 above principles.

3. Accountability

The trust and its schools 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, as amended by the DUAA, and will provide comprehensive, clear and transparent privacy information. The school will retain evidence that it complies with these requirements.

The trust will be able to demonstrate how data is processed as a whole across the MAT and will ensure each individual school within the trust is adhering to the same procedure and that this is being implemented and enforced in line with the wider trust policies.

Additional internal records of the school's processing activities will be maintained and kept up to date on the school's Data Map.

Internal records of processing activities will be recorded on the trust's Data Asset Register and 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 trust and its schools will also document other aspects of compliance with the UK GDPR and DPA where this is deemed appropriate in certain circumstances by the DPO, 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
- Records of data protection complaints, including receipt, acknowledgement, enquiries, progress updates, outcomes and remedial action.
- Decisions to rely on recognised legitimate interests, including the applicable condition and why the processing is necessary.

- Records of significant decisions based solely on automated processing, including the lawful basis and safeguards applied.

The trust and its schools 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.

4. Data protection officer (DPO)

The trust is required to appoint a DPO who will be the central point of contact for all data subjects and others in relation to matters of data protection.

A DPO will be appointed in order to:

- Inform and advise the trust, schools and employees about their obligations to comply with the UK GDPR and other data protection laws.
- Monitor the trust and its schools' 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 ICO and act as the first point of contact for the ICO 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 trust and its schools' 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 trust 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.

- Monitoring the school's handling of data protection complaints and advising on the complaints process.
- Advising on the use of recognised legitimate interests and significant automated decision-making.
- Supporting staff training so that information rights requests and data protection complaints are recognised and referred promptly.

The individual appointed as 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 trust, which is the Board of Trustees.

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

5. Lawful processing

The legal basis for processing data will be identified and documented prior to data being processed. Under the UK GDPR, 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 school 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, i.e. 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
- Processing is necessary for a recognised legitimate interest specified in Annex 1 to the UK GDPR, namely responding to a request for disclosure for another organisation's public task or official function; national security, public security or defence; emergencies; preventing, detecting or investigating crime; or safeguarding vulnerable individuals.

Where the school relies on recognised legitimate interests, it will identify and document the applicable condition and demonstrate that the processing is necessary. Where the school is a public authority, it will not use this basis to perform its public tasks or official functions. This basis will not be used for significant decisions based solely on automated processing. Where special category or criminal offence data is involved, the school will also identify an appropriate additional condition.

Where a lawful basis requires processing to be necessary, the school will ensure that the purpose cannot reasonably be achieved by less intrusive means or by processing less personal data. Consent will not be treated as the default lawful basis where another basis is more appropriate.

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 school 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 explicit details:

- Why the school needs to collect personal data

- The lawful basis relied upon and, where recognised legitimate interests is used, the applicable condition.
- What the school plans to do with the personal data
- How long the school will keep the personal data
- Whether the school 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 school's DPO at least annually and whenever significant changes are made to how the school processes the data that it collects.

The school will ensure that any parents, pupils and staff whose personal data is included will be notified of any significant changes to the privacy notice or the way in which the school 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 to make a data protection complaint to the school and to complain to the ICO in relation to the processing.

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

- **School workforce**
- **Trustees and governors**
- **Pupils, parents and guardians**
- **Occupational Health Referrals**
- **Referees**
- **Prospective employees**

There may be circumstances where it is considered necessary to process personal data or special category personal data in order 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 DPO will be consulted and a decision made only after seeking further clarification.

Where the school relies on:

- 'Performance of contract' to process a child's data, the school considers the child's competence to understand what they are agreeing to, and to enter into a contract.
- 'Legitimate interests' to process a child's data, the school takes responsibility for identifying the risks and consequences of the processing, and puts age-appropriate safeguards in place.

- 'Recognised legitimate interests' to process a child's data, the school identifies the applicable condition, demonstrates necessity, and puts age-appropriate safeguards in place.
- Consent to process a child's data, the school ensures that the requirements outlined in the 'Consent' section are met, and the school does not exploit any imbalance of power in the relationship between the school and the child.

.

6. Consent

Consent must be a positive indication expressly confirmed in words. 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 trust and its schools ensure 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 pupils and staff join the trust or its schools, the staff member or pupil (or, where appropriate, pupil's parent) 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.

Where a school opts to provide an online service directly to a child, the child is aged 13 or over, and the consent meets the requirements outlined above, the school obtains consent directly from that child; otherwise, consent is obtained from whoever holds parental responsibility for the child, except where the processing is related to preventative or counselling services offered directly to children. In all other instances with regards to obtaining consent, an appropriate age of consent is considered by the school on a case-by-case basis, taking into account the requirements outlined above.

7. The right to be informed

Adults and children have the same right to be informed about how the trust and its schools use 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
- Where recognised legitimate interests is relied upon, the applicable recognised legitimate interest condition.
- 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
  - Make a data protection complaint to the school.
  - Lodge a complaint with the ICO.
- 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 school 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.

8. The right of access

Individuals, including children, have the right to obtain a copy of their personal data as well as other supplementary information, including confirmation that their data is being processed, and 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 trust and its schools will verify the identity of the person making the request before any information is supplied.

The school will make a reasonable and proportionate search for the requested personal data. It is not required to undertake searches that would be unreasonable or disproportionate in light of the importance of providing access to the information.

A copy of the information will be supplied to the individual free of charge; however, the trust and its schools may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual requests further copies of the same information. 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.

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

Where a SAR has been made for information held about a child, the school will evaluate whether the child is capable of fully understanding their rights. If the school determines the child can understand their rights, it will respond directly to the child.

All requests will be responded to without delay and at the latest, within one month of receiving the request. Where the school reasonably requires information to confirm the requester's identity, evidence that a third party is authorised to act, or payment of a permitted fee, the response period will begin when that information, evidence or fee is received. The period may be extended by up to two further months where necessary because the request is complex or the individual has made a number of requests The individual will be informed of any extension and the reasons within the initial one-month period.

Where a request is manifestly unfounded or excessive, the trust and its schools hold 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 trust and its schools 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 trust and its schools 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 that 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.

The school may ask the individual to clarify the personal data requested only where clarification is reasonably required to provide an effective response. The response period will pause on the day clarification is requested and resume on the day after it is received. The school will not use clarification to delay a response or require the individual to narrow an otherwise clear request; where the individual does not narrow the request, the school will still carry out a reasonable and proportionate search.

The school's response will explain the individual's right to make a data protection complaint to the school and to complain to the ICO.

9. The right to rectification

Individuals, including children, 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 trust and its schools 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 trust and its schools reserve the right to refuse to process requests for rectification if they are manifestly unfounded or excessive or if exemptions apply.

The trust and its schools 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 trust and its schools 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 trust and its schools will inform them of the rectification where possible. Where appropriate, the trust and its schools 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 trust and its schools 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.

10. The right to erasure

Individuals, including children, hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing. Individuals, including children, 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 or processed
- When the individual withdraws their consent where consent was the lawful basis on which the processing of the data relied
- 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 trust and its schools will comply with the request for erasure without undue delay and at the latest within one month of receipt of the request.

The trust and its schools have 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 establishment, exercise or defence of legal claims

The trust and its schools have the right to refuse a request for erasure for special category data where processing is necessary for:

- Public health purposes in the public interest, e.g. protecting against serious cross-border threats to health.
- Purposes of preventative or occupational medicine, the working capacity of an employee, medical diagnosis, the provision of health or social care, or the management of health or social care systems or services.

Requests for erasure will be handled free of charge; however, the trust and its schools 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.

As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

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 trust and its schools will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

11. The right to restrict processing

Individuals, including children, have the right to block or suppress the trust and its schools' processing of personal data.

The trust and its schools 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 school has verified the accuracy of the data

- Where an individual has objected to the processing and the trust and its schools are 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 trust and its schools no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

In the event that processing is restricted, the trust and its schools 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 trust and its schools will inform individuals when a restriction on processing has been lifted.

Where the trust and its schools are restricting the processing of personal data in response to a request, it will make that data inaccessible to others, where possible, e.g. by temporarily moving the data to another processing system or unpublishing published data from a website.

If the personal data in question has been disclosed to third parties, the trust and its schools 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 trust and its schools reserves the right to refuse requests for restricting processing if they are manifestly unfounded or excessive or if exemptions apply. 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.

12. The right to data portability

Individuals, including children, have the right to obtain and reuse their personal data for their own purposes across different services. The right to data portability only applies in the following cases:

- Where personal data has been provided directly by an individual 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 can be easily moved, copied or transferred from one ICT environment to another in a safe and secure manner, without hindrance to usability. Personal data will be provided in a structured, commonly used and machine-readable form. Where feasible, data will be transmitted directly to another organisation at the request of the individual. The trust and its schools will not be required to adopt or maintain processing systems which are technically compatible with other organisations.

The trust and its schools will provide the information free of charge.

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

The trust and its schools 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 trust and its schools 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.

13. The right to object

The trust and its schools will inform individuals, including children, of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information. Individuals, including children, have the right to object to the following:

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

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

- An individual's grounds for objecting must relate to his or her particular situation.
- The trust and its schools will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the school can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.
- The trust and its schools will respond to objections proportionally, granting more weight to an individual's objection if the processing of their data is causing them substantial damage or distress.

Where personal data is processed for direct marketing purposes:

- The right to object is absolute and the trust and its schools will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The trust and its schools cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.
- The trust and its schools will retain only enough information about the individual to ensure that the individual's preference not to receive direct marketing is respected in future.

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 trust and its schools are 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 trust and its schools will offer a method for individuals to object online.

The DPO will ensure that details are recorded for all objections received, including those made by telephone or in person, and will clarify each objection with the individual making the request to avoid later disputes or misunderstandings. The trust and its schools will respond to all objections without undue delay and within one month of receiving the objection; this may be extended by a further two months if the request is complex or repetitive.

Where no action is being taken in response to an objection, the trust and its schools 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.

14. Informing data subjects

The school ensures that pupils, parents and staff whose data is processed by the school are clearly and explicitly informed about how the school deals with their personal data. The privacy notice will outline the features and functions of the school's use of personal data, but the privacy notice itself must be easily accessible to all who wish to view it.

The school will share its privacy notice with pupils:

- Through the pupils' induction pack when joining the school.
- At the start of each school year.
- On the school website.

The school will share its privacy notice with staff through:

- Role application.
- Contract acceptation.
- Regular appraisal.
- The start of each school year.
- Staff notice boards and other relevant staff-centric space.

15. Information rights requests

As well as the right to rectification, the school will recognise that its pupils have information rights, meaning that they have the right to access or amend any personal information that is held about them. The most common of these are SAR.

A pupil can make an information rights request relating to any of the following:

- Changing any inaccurate information that the school holds about them
- Removing their personal information or record from the school's systems

- Restricting the school from processing any data held on the pupil
- Stopping the school from processing any personal data entirely

The school will respond to any information rights request within the applicable statutory timeframe. SAR response periods will be calculated in accordance with the 'Right of access' section of this policy, including any permitted pause while reasonably required clarification is awaited.

The school will train staff to recognise and promptly refer information rights requests and data protection complaints, and to distinguish between them and other service, grievance or safeguarding complaints.

16. Data protection complaints

A data protection complaint is an expression of concern that the school has infringed data protection legislation in the way it has collected, used, shared, stored, secured, retained or otherwise processed personal data, or in the way it has responded to an information rights request. The complainant does not need to use legal terminology, refer to legislation, or use a prescribed form in order to make a data protection complaint.

The school will provide clear and accessible ways to make a data protection complaint, including an electronic route. Current contact details and the electronic complaints route will be published on the school website and in relevant privacy notices. Complaints made verbally, in writing, by email, through social media or through any other school channel will be accepted.

Staff who receive a data protection complaint will record it and refer it without delay to the DPO or the person responsible for coordinating the response. The school will make reasonable adjustments and provide age-appropriate support, where required, and will respond urgently where a complaint raises an immediate safeguarding or security risk.

The school will:

- Acknowledge receipt of the complaint within 30 days.
- Begin making appropriate enquiries and taking appropriate steps to respond without undue delay; the investigation will not be postponed until the acknowledgement period has expired.
- Keep the complainant informed of the complaint's progress and explain any delay without undue delay.
- Communicate the outcome without undue delay, including the findings, any action taken or proposed, and the right to complain to the ICO.

Where the complainant's identity or a representative's authority is uncertain, the school will request only the information reasonably necessary to verify it and will do so promptly.

Where the data protection complaint forms part of a wider complaint, grievance or safeguarding matter, the data protection element will be handled under this section and will not be delayed unnecessarily by the wider process.

Where a complaint concerns processing carried out by a processor or joint controller, the school will coordinate with the relevant organisation under the applicable contract or arrangement while retaining responsibility for its own controller obligations.

The school will keep a proportionate record of the complaint, acknowledgement, enquiries, evidence, progress updates, outcome and remedial action in line with the Records Management Policy. The DPO will review recurring themes and trends to identify improvements.

Using the school's complaints process does not affect the individual's right to complain to the ICO or seek a judicial remedy.

17. Automated decision making and profiling

For the purposes of this policy, a decision is based solely on automated processing where there is no meaningful human involvement in taking the decision. A decision is significant where it produces a legal effect or a similarly significant effect on an individual.

The school will not make a significant decision based solely on automated processing unless it has identified and documented an appropriate lawful basis, the processing is necessary and proportionate, and the safeguards in this section are in place. Recognised legitimate interests will not be used as the lawful basis for such a decision.

Where a significant solely automated decision is based entirely or partly on special category data, it will only be made where either the decision is based entirely on processing for which the individual has given explicit consent, or both of the following apply: the decision is necessary for entering into or performing a contract, or is required or authorised by law; and the processing meets the substantial public interest condition in Article 9(2)(g) of the UK GDPR.

The school will not use solely automated processing to make a significant decision about a child.

The trust and its schools will conduct a DPIA before introducing significant solely automated decision-making and will assess accuracy, fairness, bias, discrimination, security and the particular risks to children and other vulnerable individuals

The school will ensure that safeguards are in place which:

- Provide the individual with information about the decision.
- Enable the individual to make representations about the decision.
- Enable the individual to obtain human intervention by the school.
- Enable the individual to contest the decision.

Any human review will be meaningful. The reviewer will be suitably qualified, will consider the relevant information independently, and will have authority to change or reject the automated outcome; a nominal approval will not be sufficient.

The school will not use generative AI or another automated system to determine academic grading, behaviour sanctions, admissions, safeguarding decisions or staff appraisals without meaningful human involvement.

When automatically processing personal data for profiling purposes, the trust and its schools 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.

The school will keep appropriate records of the lawful basis, system logic, personal data used, safeguards applied and any human review.

18. Data protection by design and default

The trust and its schools 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 trust and its schools have considered and integrated data protection into all aspects of processing activities. In line with the data protection by default approach, the trust and its schools will ensure that only data that is necessary to achieve its specific purpose will be processed.

Where the school provides an online service likely to be accessed by children, it will take account of children's higher protection matters when deciding which technical and organisational measures are appropriate. This includes how best to protect and support child users, the fact that children may be less aware of data protection risks, consequences and rights, and their differing needs at different ages and stages of development. The school will document how these matters have been considered when designing and operating the service.

The trust and its schools 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.

19. Data Protection Impact Assessments (DPIAs)

DPIAs will be used in certain circumstances to identify the most effective method of complying with the trust'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, particularly if the AI tool automates decision-making, involves profiling, or carries a risk of bias, inaccuracy, or data misuse.

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 trust and its schools to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the school'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 trust and its schools 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 trust will consult the ICO to seek its opinion as to whether the processing operation complies with the UK GDPR.

20. 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 will ensure that all staff are made aware of, and understand, what constitutes a data breach as part of their induction and regular refresher training. The principal will ensure staff know what action to take if they know or suspect a data breach has occurred. See Annex B for the AET internal breach reporting procedure.

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

Where the school 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 trust and its schools 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 trust and its schools 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 trust and its schools 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 trust and its schools 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.

21. 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 digital 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 will only be used to hold personal information in exceptional circumstances and if used they must be password-protected and fully encrypted. All electronic devices are password-protected to protect the information on the device in case of theft. Where possible, the trust and its schools enable electronic devices to allow the remote blocking or deletion of data in case of theft.

Where possible, staff, trustees and governors will not use their personal laptops or computers for school or trust purposes. All necessary members of staff are provided with their own secure login and password.

If staff and governors need to use their personal laptops for school or trust purposes, particularly if they are working from home, they will seek authorisation and bring their device into school before using it for work to ensure the appropriate software can be downloaded and information encrypted.

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. When sending confidential information staff will always check that the recipient is correct before sending.

Before sharing data, all staff 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.

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 trust's premises accepts full responsibility for the security of the data.

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

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

Schools will regularly test, assess and evaluate the effectiveness of any and all measures in place for data security.

The trust and its schools take their duties under the UK GDPR seriously and any unauthorised disclosure may result in disciplinary action. Principals are responsible for ensuring continuity and recovery measures are in place to ensure the security of protected data.

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

The trust and its schools will maintain a list of records that have been destroyed or permanently deleted and who authorised their destruction in accordance with the Freedom of Information Act 2000.

The trust and its schools hold 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.

Employees should be aware that they can be criminally liable if they knowingly or recklessly disclose personal information outside their employer's policies and procedures.

22. Safeguarding

The trust and its schools understand that the UK GDPR does not prevent or limit the sharing of information for the purposes of keeping children safe.

The school will identify and document the Article 6 lawful basis for safeguarding processing and, where special category or criminal offence data is involved, the relevant additional condition. Where recognised legitimate interests is relied upon, the school will document the safeguarding condition and why the processing is necessary; where acting as a public authority, the school will not use this basis to perform its public tasks or official functions.

Schools will ensure that staff have due regard to their ability to share personal information for safeguarding purposes, and that fears about sharing information must not be allowed to obstruct the need to safeguard and protect pupils. The Board of Trustees will ensure that staff are:

- Confident of the processing conditions which allow them to store and share information for safeguarding purposes, including information, which is sensitive and personal, and should be treated as 'special category personal data'.
- Aware that information can be shared without consent where there is good reason to do so, and the sharing of information will enhance the safeguarding of a pupil in a timely manner.

Schools will ensure that information pertinent to identify, assess and respond to risks or concerns about the safety of a child is shared with the relevant individuals or agencies proactively and as soon as is reasonably possible. Where there is doubt over whether safeguarding information is to be shared, especially with other agencies, the DSL will ensure that they record the following information:

- Whether data was shared
- What data was shared
- With whom data was shared
- For what reason data was shared

- Where a decision has been made not to seek consent from the data subject or their parent
- The reason that consent has not been sought, where appropriate

The school will identify and document the lawful basis for safeguarding processing and, where special-category or criminal-offence data is involved, the applicable additional condition.

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

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

23. Publication of information

Schools publish a Freedom of Information Publication Scheme on their 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.

Schools will not publish any personal information, including photos, on their website without the permission of the affected individual. When uploading information to the school's website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

24. CCTV and photography

The trust and its schools understand that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

Schools notify all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email. Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose. All CCTV footage will be kept for no longer than six months for security purposes; the principal is responsible for keeping the records secure and allowing access.

Before schools are able to obtain the data of pupils or staff, they are required to give notification and obtain consent for this Special Category Data due to additional requirements for processing such data under the Protection of Freedoms Act 2012.

The trust and its schools will always indicate their intentions for taking photographs of pupils and will retrieve permission before publishing them. If the trust and its schools wish to use images or video footage of pupils in a publication, such as the school/trust website, prospectus, or recordings of school plays, written permission will be sought for the particular usage from the parent of the pupil. Precautions, as outlined in the Photography and Images Policy, are taken when publishing photographs of pupils, in print, video or on the school/trust website.

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

Parents and others attending school events are able to take photographs and videos of those events as long as they are for domestic purposes only and there are no safeguarding reasons to prevent this. The school's DSL will always be consulted before allowing parents and others to take photographs and videos for domestic purposes. Photographs or videos being used for any other purpose are prohibited to be taken by parents or visitors to the school.

The trust and its schools ask that parents and others do not post any images or videos which include any children other than their own on any social media, or otherwise publish those images or videos.

25. Procurement and management of educational technology

For the purposes of this policy, **"EdTech"** includes digital tools and systems used to support or deliver education, learning, communication, assessment, or school administration. Any EdTech tool that processes personal data will be assessed and approved before it is purchased, trialled or introduced. The DPO will be consulted from the earliest stage and throughout implementation. The DSL and ICT lead will also be involved where safeguarding, online safety, or security risks are relevant.

Before approving an EdTech tool, the school will establish and document:

- The educational purpose of the tool and the categories of personal data it will process, including whether special category data is involved.
- Why each category of data is necessary and proportionate, ensuring that optional data fields and non-core features that are not required are disabled by default.
- The lawful basis for each processing activity and, where relevant, the condition for processing special category data.
- How personal data will flow through the service, who will have access to it, where it will be stored or processed, and whether any international transfers will take place.
- Whether the school, supplier or any other party acts as a controller, joint controller, processor, or sub-processor for each part of the service.

- Whether the tool uses AI, profiling or automated decision-making and, where it does, whether the requirements in the 'Automated decision-making and profiling' and 'Use of generative artificial intelligence (AI)' sections of this policy are met.

A DPIA will be completed before approval where the processing is likely to result in a high risk to the rights and freedoms of individuals. The school will not proceed until identified risks have been reduced to an acceptable level. The DPIA will be reviewed and updated where the tool, its features, the supplier's processing, or the categories of personal data change.

The school will undertake proportionate due diligence on the supplier and will require sufficient information to verify that the tool meets the school's data protection, security, and safeguarding requirements. This will include considering whether:

- Data protection by design and by default is built into the tool.
- Appropriate security measures are in place, including encryption, secure authentication, audit logging, and systems for detecting unusual or unauthorised activity, with suitable independent assurance where available.
- Pupil-facing services provide appropriate filtering, monitoring, moderation, and audit trails, and meet relevant age-appropriate design standards where the supplier acts as a controller or joint controller.
- The supplier can support the school in responding to information rights requests and data protection complaints, investigating incidents and demonstrating compliance.
- Where AI is used, the supplier can explain how outputs are moderated, whether personal data is used to train the model, how inaccuracies and bias are mitigated, and what controls and monitoring are available to the school.

Before personal data is shared, the school will ensure that a written contract or data processing agreement clearly allocates responsibilities and covers:

- The school's documented instructions, confidentiality requirements, and access by authorised supplier staff.
- Security measures, the use and approval of sub-processors, and any international transfer arrangements and safeguards.
- The supplier's breach notification timescales and assistance with investigation, mitigation, and reporting.
- Support for data subject rights and data protection complaints, and the school's ability to obtain, correct, restrict, erase or export data where required.
- Retention, return, and secure deletion requirements, including agreed arrangements for backups, caches, and archives.
- Audit, assurance, and compliance information required by the school.

When an approved tool is implemented, access will be limited to authorised users and only the data fields and features necessary for the agreed purpose will be enabled. Privacy notices and other information provided to pupils, parents, staff, and other users will be updated where required, and users will receive appropriate instructions or training.

The school will monitor approved EdTech tools and suppliers at planned intervals and when changes or updates are proposed. Reviews will cover security, performance, processing activities, sub-processors, new features, and contractual compliance. Features that involve additional personal data will not be enabled automatically. Where processing changes, the school will reassess the lawful basis and risks and will update the DPIA, privacy notices, and other relevant policies or information as appropriate.

At the end of a contract or when changing supplier, the school will follow an agreed exit plan. Personal data will be securely returned or transferred within agreed timescales, access will be revoked, and any remaining copies held by the supplier, including backups, caches, and archives, will be securely deleted. The school will obtain confirmation of deletion and retain an appropriate record of the completed exit process.

The school will not procure or continue using an EdTech tool where the supplier cannot provide sufficient information, meet the school's requirements, or reduce identified risks to an acceptable level.

26. 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 school 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 school will ensure that the provider demonstrates UK GDPR compliance, provides explicit guarantees regarding non-retention of input data, and allows the school 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 the school.

All files and personal data will be encrypted before they leave a school 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/trust devices, only authorised parties will be able to access files on the cloud. An audit process will be put in place to alert the trust and its schools should unauthorised access, deletion or modification occur, and ensure ongoing compliance with the trust and its schools' policies for the use of cloud computing.

The trust and its schools' usage of cloud computing, including the service's security and efficiency, will be assessed and monitored by the DPO. The DPO 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 DPO 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 trust'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 trust or its schools 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 trust or its schools are prepared to accept that risk.
- Monitor the use of the trust and its schools' cloud service, with any suspicious or inappropriate behaviour of pupils, staff or parents being reported directly to the principal.

27. Use of generative artificial intelligence (AI)

The school recognises that generative AI technologies involve the processing of extensive datasets and may pose increased risks to data privacy and security.

Staff and pupils must not input personal, identifiable, or sensitive data into generative AI platforms unless the system has been formally assessed, and explicit approval has been granted following a full DPIA.

Only AI systems that meet UK GDPR standards and have been assessed for data minimisation, security, transparency, and retention practices will be used in school operations.

Use of generative AI tools must comply with the school's Acceptable Use Policy. Individuals must not rely solely on AI-generated outputs without appropriate human oversight and validation.

Any incidents, breaches, or concerns arising from the use of AI tools must be reported immediately to the DPO and will be investigated in line with the school's data breach procedures.

28. 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 pupils or employees of the school 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. The trust and its schools will refer to the trust's Records Management Policy for guidance on retention periods.

29. 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.

30. Monitoring and review

This policy is reviewed by the DPO in accordance with the trust's policy review schedule.

Annex A - AET Subject Access Request Procedure

If somebody asks you for a copy of the personal information being held by the school or trust about them you should always take action

1. Inform your principal or line manager who should then inform the trust's Data Protection Officer (DPO) that a SAR has been received. The request will be logged to ensure we comply with data protection legislation.
2. Appoint a SAR handler.
3. Acknowledge you've received the subject access request as soon as possible. Tell the requester when you'll send the response.
4. Make sure it is clear from the request exactly what personal data the individual wants. Ask for clarification if you need to.
5. Check the identity of the requester and their right to request the data. You may ask to see ID.
6. Consider if the subject access request is complex by consulting the ICO guidance. If it is and you need another 2 months to produce the information, make sure you've told the requester within one month of receiving the request. You must explain why you need the extra 2 months.
7. Search all electronic and physical locations where the requested data may be being processed. Your school's data map can help identify where information may be.
8. You should consider whether it is possible to comply with the request without disclosing information that identifies another individual . You may be able to redact information about third-parties in order to comply with the request.
9. If this is not possible, you do not have to comply with the request except where the other individual consents to the disclosure or it is reasonable to comply with the request without that individual's consent. In these circumstances contact the trust's DPO as you'll need to look at guidance for further information on what you need to consider in these circumstances.
10. Before you send any data to the requester, carefully check it and ensure the principal authorises its disclosure.
11. Send the final response by securely transferring the requested information to the individual.

The Trust's DPO will request you complete a subject access request record form that you must return to them. This is so the request can be recorded on the trust's SAR log which we are required to maintain under UK GDPR.

Annex B - AET Data breach internal procedure to follow

Always take action if you suspect a data breach may have occurred. Some breaches may need to be reported to the ICO and the DPO must do this within 72 hours.

1. Immediately inform the school's principal or your line manager. The Trust's DPO must also be informed, contact details are ltreadway@aet.cheshire.sch.uk or dpo@aet.cheshire.sch.uk
2. Be clear about the type of personal data involved. This is an important step in understanding the seriousness of the breach. We'll need to understand as soon as possible what types of personal data are involved and who the data subjects are.
3. **As soon as possible take action to limit further impact.** The priority is to establish what has happened to the personal data. You need to find out where the personal data that has been accessed, lost or stolen is now, and who might have it. If you can recover the data, you should do so immediately. You should do whatever you can to protect those who'll be most impacted. This might include recalling or asking someone to delete an email containing personal data sent by mistake, retracing your steps or contacting reception if you have physically lost some personal data to see if it has been handed in or checking if you can lock or wipe a laptop, phone or tablet containing personal data that has been stolen remotely.
4. The DPO will ask you to accurately record all details of the breach.
5. The DPO will make an assessment of how seriously we think people might be harmed and the probability of this happening. If the risk is high, then we must inform those affected as soon as possible. We must also advise them on any steps they should take to protect themselves from the risks identified. The DPO will support with these actions.
6. After every personal data breach or near miss, the DPO will review:

- what happened
- how it happened
- why it happened
- what actions the trust can take to prevent it happening again.