Ambition Education Trust

GDPR Policy

Policy Group	E	Data, IT, GDPR and Security
Title	E1	General Data Protection Regulations
Trust sub-committee		Resources
Last reviewed		Sept 2024
Next scheduled review		Sept 2025
Co-ordinated by		Phil O'Neill

1 Introduction

1.1 This is an Ambition Education Trust (AET) Policy, but relates to all the Schools within AET. AET is the organisation which is in charge of the Trust and its School's personal information. This means that AET is called the Data Controller.

1.2 The Schools within AET are referred to in this policy as 'the School' and the AET Multi Academy Trust is referred to as 'the Trust'.

1.3 This policy sets out how we protect data and how we will respond to any suspected or actual data breaches. It should be read alongside the Trust's Data and Records Management Policy.

1.4 If there is deemed to be a "high risk" to the rights and freedoms of individuals following a data breach, the Trust/School is also required to notify the individuals affected by the breach. However, in the interests of transparency, the Trust/School recognise that on some occasions it will be appropriate to notify affected individuals, even if we are not legally obliged to do so.

1.5 Privacy Notices are also available.

2 Aims

2.1 This policy aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018).

2.2 **Responsibilities**

This policy applies to all staff employed by the Trust (including Members, Directors, Trustees and Local Governing Body Governors) and to external organisations or individuals working on the Trust's behalf. Staff are required to read and confirm that they understand this policy, this will be repeated annually at the start of the school year. Staff who do not comply with this policy may face disciplinary action.

2.3 Board of Directors

The Trust Board of Directors has overall responsibility for ensuring that the Trust and its Schools comply with all relevant data protection obligations.

2.4 Data Protection Officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on Trust data protection issues.

2.5 The DPO/DEPUTY DPO is also the first point of contact for individuals whose data the Trust processes, and for the ICO.

2.6 The Trust's DPO is Jon Ryan He can be contacted in writing at Ambition Education Trust Sandringham School, The Ridgeway, St Albans, Hertfordshire, AL4 9NX or by email on dpo@aetrust.uk

2.7 All staff

Staff are responsible for:

2.7.1 Collecting, storing and processing any personal data in accordance with this policy

2.7.2 Informing the Trust of any changes to their personal data, such as a change of address

2.7.3 Contacting the DPO/DEPUTY DPO in the following circumstances:

2.7.3.1 With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure

2.7.3.2 If they have any concerns that this policy is not being followed

2.7.3.3 If they are unsure whether or not they have a lawful basis to use personal data in a particular way

2.7.3.4 If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area

2.7.3.5 If there has been a data breach
2.7.3.6 Whenever they are engaging in a new activity that may affect the privacy rights of individuals
2.7.3.7 If they need help with any contracts or sharing personal data with third parties

2.8 The DPO/DEPUTY DPO is contacted by the above party/parties as required. The DPO/ Deputy DPO by school is as follows:

2.8.1 Ridgeway Academy: Louise Jesson (Deputy DPO)
2.8.2 Verulam School: Nene Destickere (Deputy DPO)
2.8.3 Sandringham School: Andy Cracknell (Deputy DPO)
2.8.4 Wheatfields Junior School: Janice Tearle (Deputy DPO),
2.8.5 Wheatfields Infants' and Nursery School: Clare Cockburn (Deputy DPO) Dorothy Murray (DPO)
2.8.6 Garden Fields JMI: Paul Sutton (Deputy DPO)
2.8.7 Skyswood Primary & Nursery School: Robert Bridle (Deputy DPO)
2.8.8 The Adeyfield Academy – Awandja Ebhodaghe (Deputy DPO)
2.8.9 St Albans Girls School – Ben Young (Deputy DPO)
2.8.10 Beech Hyde Primary and Nursery School – Jon Ryan

2.9 **<u>Members, Trustees and LGB Governors</u>**
Members, Trustees and LGB Governors must inform the Trust of any changes to their personal data, such as a change of address.

3 Collecting Data

3.1 The Trust collects and uses certain types of personal information about staff, students, parents and other individuals who come into contact with the Trust in order to provide education and associated functions. The Trust may be required by law to collect and use certain types of information to comply with statutory obligations related to employment, education and safeguarding, and this policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the General Data Protection Regulation and other related legislation.

3.2 GDPR applies to all computerised data and manual files if they come within the definition of a filing system. Broadly speaking, a filing system is one where the data is structured in some way that it is searchable on the basis of specific criteria (for example using the individual's name to find their information), and if this is the case, it does not matter whether the information is located in a different physical location.

3.3 This policy will be updated as necessary to reflect best practice, or amendments made to data protection legislation, and shall be reviewed annually.

3.4 **<u>School Holidays</u>**

3.4.1 The Trust recognises that there are times throughout the year when our ability to identify and respond to a breach swiftly and robustly may be impeded because schools are closed and may have limited staff available during this time. A breach may still occur during these periods and we will implement the following steps to mitigate any risk caused if a breach happens during school holidays:
3.4.2 The DPO@ email address will be made available to staff and will be available on the Trust website and in our main Privacy Notice, so that a member of staff can be alerted, should an incident occur. This email address will be monitored regularly.
3.4.3 The Deputy DPO will have the contact details for appropriate staff and support, so that action can be taken without delay should a breach occur.
3.4.4 The Deputy DPO should follow the steps set out above as best as he / she can in the circumstances. In particular, this should include reporting notifiable breaches to the ICO within 72 hours and, if required, the affected individuals. The report to the ICO should state that schools are closed and limited staff available due to the holidays and, depending on the circumstances, advice should be sought from the ICO on the steps the Trust/School should take to mitigate any risks.

4 Personal Data

4.1 Personal data is information that identifies an individual, and includes information that would identify an individual to the person to whom it is disclosed because of any special knowledge that they have or can obtain. A subset of personal data is known as 'special category data'. This special category data is information that relates to:

- 4.1.1 race or ethnic origin
- 4.1.2 political opinions
- 4.1.3 religious or philosophical beliefs
- 4.1.4 trade union membership
- 4.1.5 physical or mental health
- 4.1.6 an individual's sex life or sexual orientation
- 4.1.7 genetic or biometric data for the purpose of uniquely identifying a natural person

4.2 Special category data is given special protection, and additional safeguards apply if this information is to be collected and used.

4.3 Information related to criminal convictions shall only be held and processed where there is legal authority to do so.

4.4 The Trust does not intend to seek or hold special category data (previously known as sensitive personal data) about staff or students except where the Trust has been notified of the information, or it comes to the Trust's attention via legitimate means (e.g. a grievance) or needs to be sought and held in compliance with a legal obligation or as a matter of good practice. Staff or students are under no obligation to disclose to the Trust their race or ethnic origin, political or religious beliefs, whether or not they are a trade union member or details of their sexual life (save to the extent that details of marital status and / or parenthood are needed for other purposes, e.g. pension entitlements). Further information relating to criminal offences/convictions and processing such information also requires additional safeguards, separate to those in relation to special category data as detailed above.

5 The Data Protection Principles

5.1 The six data protection principles as laid down in the GDPR are followed at all times:

- 5.1.1 personal data shall be processed fairly, lawfully and in a transparent manner, and processing shall not be lawful unless one of the processing conditions can be met
- 5.1.2 personal data shall be collected for specific, explicit, and legitimate purposes, and shall not be further processed in a manner incompatible with those purposes (purpose limitation)
- 5.1.3 personal data shall be adequate, relevant, and limited to what is necessary for the purpose(s) for which it is being processed (data minimisation)
- 5.1.4 personal data shall be accurate and, where necessary, kept up to date
- 5.1.5 personal data processed for any purpose(s) shall not be kept in a form which permits identification of individuals for longer than is necessary for that purpose / those purposes (storage limitation)
- **5.1.6** personal data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures

5.2 In addition to this, the Trust is committed to ensuring that at all times, anyone dealing with personal data shall be mindful of the individual's rights under the law (as explained in more Detail below).

5.3 The Trust is also responsible for, and is committed to demonstrating compliance with the above data protection principles at all times (accountability). This means that the Trust will:

5.3.1 inform individuals about how and why we process their personal data through the Privacy Notices which we issue
5.3.2 be responsible for checking the quality and accuracy of the information
5.3.3 regularly review the records held to ensure that information is not held longer than is necessary, and that it has been held in accordance with the Records Retention Policy
5.3.4 ensure that when information is authorised for disposal it is done appropriately
5.3.5 ensure appropriate security measures to safeguard personal information whether it is held in paper files or on our computer system, and follow the relevant Security Policy requirements at all times
5.3.6 share personal information with others only when it is necessary and legally appropriate to do so
5.3.7 set out clear procedures for responding to requests for access to personal information known as subject access requests and other rights exercised by individuals in accordance with the GDPR
5.3.8 report any breaches of the GDPR in accordance with the guidelines.
5.3.9 ensure all staff are aware of and understand our policies and procedures

6 Conditions for Processing in the first Data Protection Principle

The Trust will only process personal data where it is able to rely on one of the following legal bases set out in Article 6 GDPR:

6.1 The individual has given consent that is specific to the particular type of processing activity, and that consent is informed, unambiguous and freely given.
6.2 The processing is necessary for the performance of a contract, to which the individual is a party, or is necessary for the purpose of taking steps with regards to entering into a contract with the individual, at their request.
6.3 The processing is necessary for the performance of a legal obligation to which we are subject
6.4 The processing is necessary to protect the vital interests of the individual or another.
6.5 The processing is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in us.
6.6 The processing is necessary for the legitimate interest as a legal basis for processing data.
6.7 If the personal data being processed is 'special category data', the Trust will also identify an appropriate condition exemption in accordance with Article 9 GDPR
6.8 if the personal data being processed relates to criminal convictions and offences, or related security measures ('criminal offence data') the Trust will also comply with Article 10 GDPR.

7 Use of Personal Data by the Trust

7.1 The Trust processes personal data on students, staff and other individuals such as visitors. In each case, the personal data must be processed in accordance with the data protection principles as outlined above.
7.2 **Students**
7.2.1 The personal data held regarding students includes contact details, assessment / examination results, attendance information, characteristics such as ethnic group, special educational needs, any relevant medical information, and photographs. The student privacy notice can be found here.
7.2.2 The data is used in order to support the education of the students, to monitor and report on their progress, to provide appropriate pastoral care, and to assess the progression of the Trust as a whole, together with any other uses normally associated with this provision in a school environment.
7.2.3 The Trust may make use of limited personal data (such as contact details) relating to students, and their parents or guardians for fundraising, marketing or promotional

purposes and to maintain relationships with students of the School, but only where consent has been provided for this.

7.2.4 In particular, the Trust may:

7.2.4.1 transfer information to any association society or club set up for the purpose of maintaining contact with students or for fundraising, marketing or promotional purposes relating to the Trust but only where consent has been obtained first

7.2.4.2 make personal data, including special category data, available to staff for planning curricular or extracurricular activities

7.2.4.3 keep the student's previous school informed of his / her academic progress and achievements e.g. sending a copy of the school reports for the student's first year at the School to their previous school; Use photographs of students in accordance with the Photograph Policy.

7.2.5 Any wish to limit, restrict, or object to any use of personal data should be notified to the Trust Chief Operating Officer in writing, which notice will be acknowledged by the Trust in writing. If, in the view of the Trust Chief Operating Officer, the objection cannot be maintained, the individual will be given written reasons why the Trust cannot comply with their request.

7.3 Staff

7.3.1 The personal data held about staff will include contact details, employment history, information related to DBS checks, information relating to career progression, photographs, occupational pensions, next of kin, medical information, bank account details, national insurance number etc for payroll, car registration number. The staff privacy notice can be found here .

7.3.2 The data is used to comply with legal obligations placed on the Trust in relation to employment, and the education of children in a school environment. The Trust may pass information to other regulatory authorities where appropriate, and may use names and photographs of staff in publicity and promotional material. Personal data will also be used when giving references.

7.3.3 Staff should note that information about disciplinary action may be kept for longer than the duration of the sanction. Although treated as "spent" once the period of the sanction has expired, the details of the incident may need to be kept for a longer period.

7.4 Information relating to DBS checks

7.4.1 DBS checks are carried out on the basis of the Trust's legal obligations in relation to safer recruitment of Staff as stipulated in the Independent School Standards Regulations and the DBS information (which will include personal data relating to criminal convictions and offences) is further processed in the substantial public interest, with the objective of safeguarding children. Retention of the information is covered by the Records Retention Policy which is frequently reviewed to make sure the retention periods are consistent with GDPR laws and regulations.

7.4.2 Access to the DBS information is restricted to those staff who have genuine need to have access to it for their job roles. In addition to the provision of the GDPR and the Data Protection Act 2018, disclosure of this information is restricted by section 124 of the Police Act 1997 and disclosure to third parties will only be made if it is determined to be lawful. Any wish to limit or object to the uses to which personal data is to be used should be notified to the Trust Chief Operating Officer who will ensure that this is recorded, and adhered to if appropriate. If the Trust Chief Operating Officer is of the view that it is not appropriate to limit the use of personal data in the way specified, the individual will be given written reasons why the Trust cannot comply with their request.

7.5 Other Individuals

The Trust may hold personal information in relation to other individuals who have contact with the School, such as volunteers and guests. Such information shall be held only in accordance with

the data protection principles, and shall not be kept longer than necessary. This information can be found in the privacy notice for visitors here.

8 Security of Personal Data

8.1 The Trust will take reasonable steps to ensure that members of staff will only have access to personal data where it is necessary for them to carry out their duties. All staff will be made aware of the GDPR Policy and their duties under it. The Trust will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

8.2 For further details regarding security of IT systems, please refer to the ICT Policy.

9 Disclosure of Personal Data to Third Parties

9.1 The following list includes the most usual reasons that the Trust will authorise disclosure of personal data to a third party:

- 9.1.1 to give a confidential reference relating to a current or former employee, volunteer or student for the prevention or detection of crime
- 9.1.2 for the assessment of any tax or duty
- 9.1.3 where it is necessary to exercise a right or obligation conferred or imposed by law upon the Trust (other than an obligation imposed by contract)
- 9.1.4 for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings)
- 9.1.5 for the purpose of obtaining legal advice
- 9.1.6 for research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress)
- 9.1.7 to publish the results of public examinations or other achievements of students of the Trust
- 9.1.8 to disclose details of a student's medical condition where it is in the student's interests to do so and there is a legal basis for doing so, for example for medical advice, insurance purposes or to organisers of school trips. The legal basis for this will vary in each case but will usually be based on explicit consent, the vital interests of the child or reason of substantial public interest (usually safeguarding the child or other individuals)
- 9.1.9 to provide information to another educational establishment to which a student is transferring
- **9.1.10** to provide information to the Examination Authority as part of the examination process; and to provide information to the relevant Government Department concerned with national education. At the time of the writing of this Policy, the Government Department concerned with national education is the Department for Education (DfE). The Examination Authority may also pass information to the DfE.

9.2 The DfE uses information about students for statistical purposes, to evaluate and develop education policy and to monitor the performance of the nation's education service as a whole. The statistics are used in such a way that individual students cannot be identified from them. On occasion the DfE may share the personal data with other Government Departments or agencies strictly for statistical or research purposes.

9.3 The Trust may receive requests from third parties (i.e. those other than the data subject, the School, and employees of the Trust) to disclose personal data it holds about students, their parents or guardians, staff or other individuals. This information will not generally be disclosed unless one of the specific exemptions under data protection legislation which allow disclosure applies; or where necessary for the legitimate interests of the individual concerned or the Trust.

9.4 All requests for the disclosure of personal data must be sent to the Trust Chief Operating Officer, who will review and decide whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of that third party before making any disclosure.

10 Confidentiality of Student Concerns

Where a student seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents or guardian, the Trust will maintain confidentiality unless it has reasonable grounds to believe that the student does not fully understand the consequences of withholding their consent, or where the Trust believes disclosure will be in the best interests of the student or other students. Disclosure for a public safeguarding purpose will be lawful because it will be in the substantial public interest.

11 Subject Access Requests

11.1 Anybody who makes a request to see any personal information held about them by the Trust is making a subject access request. All information relating to the individual, including that held in electronic or manual files should be considered for disclosure, provided that they constitute a "filing system". A subject access request must be made in writing to the Trust. The Trust should send all requests to the Trust Chief Operating Officer within 3 working days of receipt. The Trust Chief Operating Officer must deal with the request in full without delay and at the latest within one month of receipt to the Trust Chief Operating Officer unless the Trust requires an extension due to the request being complex or if it has received repeated requests. The Trust may ask for any further information reasonably required to locate the information.

11.2 Where a child or young person lacks capacity to understand their rights and the implications of making a subject access request (e.g. due to their age or some other reason) a third party, such as a parent or carer, can make a request on their behalf. The Trust Chief Operating Officer must, however, be satisfied that:

11.2.1 the child or young person lacks sufficient understanding; and

11.2.2 the request made on behalf of the child or young person is in their interests

11.3 Access to records will be refused in instances where an exemption applies, for example, where information sharing may place an individual at risk of significant harm or jeopardise police investigations into any alleged offence(s).

11.4 An individual only has the automatic right to access information about themselves, and care needs to be taken not to disclose the personal data of third parties where consent has not been given, and it would be unreasonable to release the information without consent.

11.5 Particular care must be taken in the case of any complaint or dispute to ensure confidentiality is protected. All files must be reviewed by the Trust Chief Operating Officer/Head Teacher before any disclosure takes place. Access will not be granted before this review has taken place.

11.6 Where all the data in a document cannot be disclosed a permanent copy should be made and the data obscured or retyped if this is more sensible. A copy of the full document and the altered document should be retained, with the reason why the document was altered.

12 Internal SAR Process Flowchart

Request is made to school or DPO/DEPUTY DPO directly

Request is sent over to DPO/DEPUTY DPO

DPO/DEPUTY DPO confirms receipt of request to requester and notifies COO and Headteacher of requested school. The DPO/DEPUTY DPO will detail the required timeline for receipt of redacted data to be sent to the requester

---

Headteacher delegates staff member as lead for data collection tasks for SAR

Lead of data collection assigns staff to areas within their role to compile data into central folder

---

Lead of each area of data collection redacts their area of the SAR Headteacher reviews all information before data pack is shared with requester

---

Lead of data collection is in charge of delivery to requester

---

Delivery confirmation sent to Headteacher, DPO/DEPUTY DPO and COO

13 Exemptions to Access by Data Subjects

13.1 Where a claim to legal professional privilege could be maintained in legal proceedings, the information is likely to be exempt from disclosure unless the privilege is waived.

13.2 There are other exemptions from the right of subject access. If we intend to apply any of them to a request, then we will clearly explain which exemption is being applied and why, wherever possible.

14 Other Rights of Individuals

14.1 The Trust has an obligation to comply with the rights of individuals under the law, and takes these rights seriously. The following section sets out how the Trust will comply with the rights to:

14.1.1 object to processing

14.1.2 rectification

14.1.3 erasure; and

14.1.4 data portability

14.2 <u>Right to object to processing</u>

14.2.1 An individual has the right to object to the processing of their personal data for direct marketing purposes. This right is absolute and where such an objection is made the Trust will stop processing personal data for this purpose.

14.2.2 An individual also has the right to object to the processing of their personal data on the grounds of pursuing public interest or legitimate interest, where they do not believe that those grounds are adequately established.

14.2.3 Where such an objection is made, it must be sent to the Trust Chief Operating Officer within 2 working days of receipt, and the Trust Chief Operating Officer will assess whether there are compelling legitimate grounds to continue processing which override the interests, rights and freedoms of the individuals, or whether the information is required for the establishment, exercise or defence of legal proceedings.

14.2.4 The Trust Chief Operating Officer shall be responsible for notifying the individual of the outcome of their assessment within ten working days of receipt of the objection.

14.3 <u>Right to rectification</u>

14.3.1 An individual has the right to request the rectification of inaccurate data without undue delay and at the latest within one calendar month. Where any request for rectification is received by the Trust, it should be sent to the Trust Chief Operating Officer within 2 working days of receipt. Where adequate proof of inaccuracy is given, the data shall be amended as soon as reasonably practicable and within one calendar month and the individual notified.

14.3.2 Where there is a dispute as to the accuracy of the data, the request and reasons for refusal shall be noted alongside the data, and communicated to the individual. The individual shall be given the option of a review under the Data Protection Complaints Procedure, or an appeal direct to the Information Commissioner.

14.3.3 An individual also has a right to have incomplete information completed by providing the missing data, and any information submitted in this way shall be updated without undue delay.

14.4 Right to erasure

14.4.1 Individuals have a right, in certain circumstances, to have data permanently erased without undue delay. This right arises in the following circumstances:

14.4.1.1 where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed

14.4.1.2 where consent is withdrawn and there is no other legal basis for the processing

14.4.1.3 where an objection has been raised under the right to object, and found to be legitimate and there is no overriding legitimate interest to continue processing

14.4.1.4 where personal data is being unlawfully processed (usually where one of the conditions for processing cannot be met)

14.4.1.5 where there is a legal obligation on the Trust to delete

14.4.2 The Trust Chief Operating Officer will make a decision regarding any application for erasure of personal data, and will balance the request against the exemptions provided for in the law. Where a decision is made to erase the data, and this data has been passed to other data controllers, and / or has been made public, reasonable attempts to inform those controllers of the request shall be made.

14.5 Right to restrict processing

In the following circumstances, processing of an individual's personal data may be restricted:

14.5.1 where the accuracy of data has been contested, during the period when the Trust is attempting to verify the accuracy of the data

14.5.2 where processing has been found to be unlawful, and the individual has asked that there be a restriction on processing rather than erasure

14.5.3 where data would normally be deleted, but the individual has requested that their information be kept for the purpose of the establishment, exercise or defence of a legal claim

14.5.4 where an individual has exercised their right to object to the processing of personal data, pending the outcome of any decision

14.6 Right to portability

If an individual wants to send their personal data to another organisation they have a right to request that the Trust provides their information in a structured, commonly used, and machine-readable format. As this right is limited to situations where the Trust is processing the information on the basis of consent or performance of a contract, the situations in which this right can be exercised will be quite limited. If a request for this is made to the Trust, it should be sent to the Trust Chief Operating Officer within 2 working days of receipt, and the Trust Chief Operating Officer will review and revert as necessary.

15 Personal Data Breaches

15.1 A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data including where data is entered into generative AI such as Chat GPT or similar. Any personal data breach shall be reported as soon as it is discovered, to the Trust Chief Operating Officer. In the absence of the COO please report directly to the DPO/DEPUTY DPO either by phone or email to dpo@aetrust.uk and this will be picked up as soon as possible.

15.2 Staff members are expected to attempt to locate the DPO/DEPUTY DPO directly or communicate with the DPO/DEPUTY DPO over the phone, if it is not possible to locate the DPO/DEPUTY DPO or COO the IT Support team at each site will be in a position to make contact with the DPO/DEPUTY DPO on your behalf or be able to direct you to where the DPO/DEPUTY DPO current is. Once notified, the Trust Chief Operating Officer shall assess:

15.1.1 the extent of the breach

15.1.2 the risks to the data subjects as a consequence of the breach

15.1.3 any security measures in place that will protect the information
15.1.4 any measures that can be taken immediately to mitigate the risk to the individuals

15.3 Unless the Trust Chief Operating Officer concludes that there is unlikely to be any risk to individuals from the breach, it must be notified to the Information Commissioner's Office within 72 hours of the breach having come to the attention of the Trust, unless a delay can be justified.

15.4 The Information Commissioner shall be told:
15.4.1 details of the breach, including the volume of data at risk, and the number and categories of data subjects
15.4.2 the contact point for any enquiries (which shall usually be the Trust Chief Operating Officer)
15.4.3 the likely consequences of the breach
15.4.4 measures proposed or already taken to address the breach

15.5 If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals then the Trust Chief Operating Officer shall notify data subjects of the breach without undue delay unless the data would be unintelligible to those not authorised to access it, or measures have been taken to mitigate any risk to the affected individuals.
Data subjects shall be told:
15.5.1 the nature of the breach
15.5.2 who to contact with any questions
15.5.3 measures taken to mitigate any risks

15.6 The Trust Chief Operating Officer shall then be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented. Any recommendations for further training or a change in procedure shall be reviewed by the board and a decision made about implementation of those recommendations.

16 Contact

If anyone has any concerns or questions in relation to this policy they should contact the Trust Chief Operating Officer.

17 Monitoring

The Trust monitors and reviews its policies and procedures on a regular basis to ensure that there is compliance.

Ambition
Education Trust

www.ambitioneducationtrust.org