Ambition Education Trust

AET Privacy Notice for Trust Staff, Trustees/Governors & Volunteers

Policy Group	E	Data, IT, GDPR & Security
Title	E1p app	AET Privacy Notice for Trust Staff, Trustees/Governors & Volunteers
Trust sub-committee		Resources
Last reviewed		October 2024 (updated June 2.25 – insert new section 6)
Next scheduled review		October 2028 (review date updated Sept 25)
Co-ordinated by		Director of IT

1 General Data Protection Regulations 2018

We, the Ambition Education Trust (AET) are data controllers for the purposes of the General Data Protection Regulations (GDPR). Where the term 'staff' is used within this policy, for safeguarding and/or data protection purposes, this can also apply to other individuals working and volunteering within the school.

2 Why do we Collect and use your Information?

2.1 We will only use your personal information where the law allows us to. Under Article 6 of the General Data Protection Regulation (GDPR), we collect and use information because we are legally required to collect some information about staff, trustees, governors and volunteers and we need to process this information due to our **legal obligation** to keep relevant and/or employment records. In addition, due to the safeguarding requirements of our school, we also collect information for the reason of **vital interest**: the processing is necessary to protect someone's life.

2.2 Normally, we will hold data due to a contract between the Trust/School and our staff as employees.

2.3 Under Article 6 and Article 9 of GDPR, where the above lawful basis does not allow us to collect essential personal information, we will use **explicit consent** or because the processing is necessary to protect the **vital interest** of the data subject, including CCTV footage where installed (see separate CCTV policy. Explicit consent would be sought if biometric data was ever to be collected/used by any of our schools.

3 How do we use your Information?

3.1 We process personal data relating to those we employ to work at, or otherwise engage within the Trust. This is for employment purposes to assist in the running of the school (the reason for Lawful Basis) and/or to enable individuals to be paid or contacted. It could include all legal matters of employment in addition to necessary safeguarding, performance, training, sickness, and grievance information.

3.2 The collection of this information will benefit both national and local users by:

- 3.2.1 improving the management of workforce data
- 3.2.2 enabling development of a comprehensive picture of the workforce/volunteers and they are deployed
- 3.2.3 appropriately informing the public about our workforce/volunteers
- 3.3.4 informing the development of recruitment and retention policies
- 3.3.5 allowing better financial modelling and planning
- 3.3.6 enabling ethnicity and disability monitoring; and
- 3.3.7 supporting the work of the School Teachers' Review Body
- 3.3.8 to ensure that the school can provide an effective education (e.g. video conferencing)

3.3 The data we keep on a Lawful Basis includes personal data identifiers such as contact details, National Insurance numbers, characteristics such as ethnic group, employment contracts and remuneration details, qualifications and absence information. Some of this data is retained due to legal requirements and some as a requirement of the Single Central Record. Some key information is contained within the required Emergency Response Plan. After you leave us, we will keep data no longer than that required by law and/or the recommendation from the local authority. If you require more information about how we and/or DfE store and use your personal data, please see the end of this document for further details.

4 Categories of Information that we Collect, Hold and Share

Any relevant information for employment purposes, including personal details (such as name and address), personal characteristics (such as ethnicity, language, nationality **if** required by the Single Central Record), information about your contract, absence, qualifications and any other specific information regarding specific needs, including relevant medical information. CCTV has been installed

at some of our schools and is used for safeguarding purposes.

5 Collecting this Information

We collect personal information about employees, workers and contractors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, the local authority or other background check agencies. To comply with the General Data Protection Regulations, we will inform you if you have a choice in this. We will also collect additional personal information throughout the period of you working for us.

6 Use of AI Technologies

The school may use AI-assisted technologies for administrative and educational purposes. For details on how AI is applied and safeguards in place, please see our AI policy.

7 Storing Data

We will hold the data for as long as we are required to by law but not longer than is recommended by the local authority. An annual sweep of the school network will be used to ensure that such data is protected and removed from general access where appropriate. Data is backed up onsite daily and offsite. This is organised by the Central AET IT Team. Data held is held on external databases only when necessary and such databases will have been checked for alignment to GDPR.

8 Who do we Share your Information with?

We will not give information about you to anyone without your consent unless the law and our policies allow us to. We may transfer your personal information outside national borders to comply with the law. If we do, you can expect a similar degree of protection in respect of your personal information.

9 Why we Share Information

9.1 We are required to provide certain information to HMRC and Schools Pension Company to maintain staff employment within the Trust or its schools. We will need to release information to the Police during investigations if they make a request.

9.2 The following activities are often but not always carried out by third-party service providers:

- 9.1.1 payroll
- 9.1.2 pension administration
- 9.1.3 benefits provision and administration
- 9.1.4 Safeguarding purposes
- 9.1.5 We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you, where it is needed in the public interest or for official purposes, or where we have your consent.

10 Department for Education

10.1 We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding/expenditure and the assessment educational attainment.

10.2 We are required to share information with the Department for Education (DfE) under regulation 7 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 as amended.

11 If you Fail to Provide Personal Information

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented

from complying with our legal obligations (such as to ensure the health and safety of our workers) or we may be unable to discharge our obligations which may be in the public interest or for official purposes.

12 Change of Purpose

12.1 We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

12.2 Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

13 How we use Particularly Sensitive Personal Information

13.1 "Special categories" of particularly sensitive personal information require us to ensure higher levels of data protection. We need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the following circumstances:

13.1.1 in limited circumstances, with your explicit consent.

13.1.2 where we need to carry out our legal obligations and in line with our data protection policy.

13.1.3 where it is needed in the public interest, such as for equal opportunities monitoring (or in relation to our occupational pension scheme), and in line with GDPR.

13.1.4 where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.

13.2 Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public. We may also process such information about members or former members in the course of legitimate business activities with the appropriate safeguards.

14 Our Obligations as an Employer

14.1 We will use particularly sensitive personal information in the following ways:

14.1.1 we will use information relating to leaves of absence including the reasons for the leave, which may include sickness absence or family-related leave, sabbaticals, to comply with employment and other laws.

14.1.2 we will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to comply with the Equality Act 2010, to monitor and manage sickness absence and to administer benefits.

14.1.3 we will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

14.1.4 we may use trade union membership information to pay trade union subscriptions, register the status of a protected employee and to comply with employment law obligations.

14.2 **Do we need your consent?**

14.2.1 We do not need your consent if we use your particularly sensitive information in accordance with our written policy where processing is necessary:

14.2.1.1 to carry out our legal obligations or exercise specific rights in the field of employment law;

14.2.1.2 for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

14.2.1.3 to share information with HCC Governance support and Governor Hub or its equivalent;

14.2.1.4 for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and we provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

14.2.2 In other circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent.

14.2.3 You should be aware that it is not a condition of a contract of employment with us that staff agree to any request for consent from us.

15 Information about Criminal Convictions

15.1 We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations, provided we do so in line with GDPR.

15.2 Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

15.3 We envisage that we will hold information about criminal convictions, for example, if information about criminal convictions comes to light as a result of our recruitment and Disclosure and Barring Service checks, or if information about criminal convictions comes to light during your employment with us.

15.4 We will only collect information about convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us.

16 Automated Decision-Making

16.1 Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

16.1.1 Where we have notified you of the decision and given you 21 days to request a reconsideration.

16.1.2 Where it is necessary to meet our obligations under your employment contract and ensure that appropriate measures are in place to safeguard your rights.

16.1.3 In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

16.2 If we make an automated decision on the basis of any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights.

16.3 You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have

notified you.

16.4 We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

17 Working from Home

17.1 In the event of staff being instructed to work from home due to a school closure, through management or government instruction, data required to do their job effectively may be taken home. It is preferred that this data is stored on a school device/network, however, any data taken/copied in any format should be protected adequately from other members of the household and from theft (stored safely and securely when not in use). Any data not required at home when usual school-based work resumes, must, under normal circumstances, be returned safely to the workplace within two weeks. Staff will be permitted to use personal devices to a greater degree than that permitted by standard policy during this time, in order to carry out work duties as necessary. Staff must adhere to the standard policy on the use of personal electronic devices when usual school operation resumes, or when extraordinary use is no longer required.

17.2 Staff may be asked to provide information to HCC and or other school related organisations in an unusual manner during a school closure/partial closure/government/business office closure.

17.3 Trust/School staff should ensure, as far as possible, that the method used to provide information, and the information itself, is in line with general GDPR practices to maintain compliance, but those methods can be adapted as required to suit any extraordinary working conditions.

17.4 Trustees (Trust) and Governors (Schools) may use any school provided or self-collated, redacted or non-redacted school data, in line with their roles and responsibilities as school governors. Volunteers may use data provided to them by senior leaders and teachers, in line with their roles, as outlined by school staff. All non-employed persons must return or destroy school data if requested by senior staff and at the termination of their roles within the school. School data should not be shared outside of expected and agreed roles without express permission of senior staff.

18 Dfe Data Collection Requirements

18.1 The following is information provided by the DfE concerning the reason it collects data about employees, trustees, governors or volunteers:

18.1.1 The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005.

18.1.2 To find out more about the data collection requirements placed on us by the DfE including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools. The DfE may share information about individuals/employees with third parties who promote the education or well-being of children or the effective deployment of school staff by:

18.1.2.1 conducting research or analysis;

18.1.2.2 producing statistics; and / or

18.1.2.3 providing information, advice or guidance

18.1.3 The DfE has robust processes in place to ensure that the confidentiality of

personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

18.1.3.1 who is requesting the data
18.1.3.2 the purpose for which it is required
18.1.3.3 the level and sensitivity of data requested
18.1.3.4 the arrangements in place to securely store and handle the data

18.2 To be granted access to school workforce information, organisations must comply with the DfE's strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

18.3 For more information about the DfE's data sharing process, please visit: https://www.gov.uk/guidance/data-protection-how-we-collect-and-share-research-data

18.4 To contact the department: https://www.gov.uk/contact-dfe

19 How Secure is your Information with Third-Party Service Providers?

All our third-party service providers are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

20 What about other Third Parties?

We may share your personal information with other third parties, for example in the context of the possible merger with another Multi Academy Trust. We may also need to share your personal information with a regulator or to otherwise comply with the law.
From time to time, we may disclose your personal data in response to a request for information pursuant to the Freedom of Information Act 2000 or following a data subject access request. We may approach you for your consent but, in any event, we will only disclose your personal data if we are satisfied that it is reasonable to do so in all the circumstances. This means that we may refuse to disclose some or all of your personal data following receipt of such a request.

21 Data Security

21.1 We have put in place measures to protect the security of your information. Details of these measures are available upon request. Third parties who are processing personal data on our behalf will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

21.2 We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions, and they are subject to a duty of confidentiality. Details of these measures may be obtained from your school on request.

21.3 We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

22 How long will we use your Information for?

22.1 To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised

use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

22.2 We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, insurance or reporting requirements.

22.3 Once you are no longer an employee, worker, contractor, volunteer, trustee or governor of the school, we will retain and securely destroy your personal information in accordance with our data retention policy **or** applicable laws and regulations. Your personal information is kept in line with national requirements. We keep employment/HR and appraisal records and financial records in line with our Trust Data and Records Management Policy or individual school policy, where different retention periods apply.

22.4 In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you.

23 Your Duty to Inform us of Changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working/voluntary relationship with us.

24 Your Rights in Connection with Personal Information

2.14 In line with the GDPR policy you have the right to the following (see bullet point list below) in respect of the data held about you. However, in certain situations such as but not restricted to the safeguarding of children, this data may not be disclosed.

24.1.1 **Request access** to your personal information (data subject access request). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.

24.1.2 **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.

24.1.3 **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).

24.1.4 **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.

24.1.5 **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.

24.1.6 **Request the transfer** of your personal information to another party.

24.2 The legal timescales for the Trust or School to respond to a subject access request is one calendar month. As the school has limited staff resources outside of term time, we encourage staff to submit subject access requests during term time and to avoid sending a request during periods when the school is closed or is about to close for the holidays, where possible. This will assist us in responding to your request as promptly as possible.

25 No Fee Usually Required

You will not usually have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is manifestly unfounded, excessive. Alternatively, we may refuse to comply with the request in such circumstances or if we have another valid reason for doing so.

26 What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

27 Right to Withdraw Consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. Inform a senior member of staff or contact the Deputy Data Protection Officer (details can be obtained from the appropriate school office). Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

28 For Further Information

28.1 This is an additional policy which relates to staff at the school. To see our general Privacy Notice, please visit the policy section of our school website.

28.2 If you want to see a copy of information about you that we hold, please contact the school office. You can contact the Trusts Deputy Data Protection officer by emailing:

- 28.2.1 Ridgeway Academy: dpo@ridgeway.aetrust.uk
- 28.2.2 Verulam School: dpo@verulam.aetrust.uk
- 28.2.3 Sandringham School: dpo@sandringham.aetrust.uk
- 28.3.4 St Albans Girls School: dpo@stags.aetrust.uk
- 28.3.5 The Adeyfield Academy: dpo@adeyfield.aetrust.uk
- 28.3.6 Wheatfields Junior School: dpo@wheatfieldsjm.aetrust.uk
- 28.3.7 Wheatfields Infants' and Nursery School: dpo@wheatfieldsinfants.aetrust.uk
- 28.3.8 Garden Fields JMI: dpo@gardenfields.aetrust.uk
- 28.3.9 Skyswood Primary & Nursery School: dpo@skyswood.aetrust.uk
- 28.3.10 Beech Hyde Primary School: dpo@beechhyde.aetrust.uk
- 28.3.11 Ambition Education Trust: dpo@aetrust.uk
- 28.3.12 You can contact the ICO at any time on 0303 123 1113 email: https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF.

28.3 Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

- 28.3.1 To find out more about your rights:
  - 28.3.1.1 https://ico.org.uk/global/privacy-notice/your-data-protection-rights/
  - 28.3.1.2 https://www.gov.uk/guidance/data-protection-how-we-collect-and-share-research-data
- 28.3.2 To find out more about school governance in Hertfordshire:
  - 28.3.2.1 https://www.hertfordshire.gov.uk/about-the-council/volunteering/schools-and-youth-work/school-

governor/school-governors.aspx
28.3.2.2 governance@hfleducation.org.

29 POLICY REVIEW – GDPR

This policy will be reviewed in full by Trustees every three years. We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

The policy was last reviewed and agreed by the Board October 2024

Name ……

Signature ……

Date ……

CEO

Name ……

Signature ……

Date ……

Chair of Trustees

Ambition
Education Trust