



Privacy Notice for the Workforce

How we use workforce information

Version	September 2026
Next review	September 2027
Data Controller	St Thomas Aquinas Catholic Multi-Academy Trust

This notice explains how the Trust collects, uses, stores and shares personal information about members of its workforce.

1. Who we are

St Thomas Aquinas Catholic Multi-Academy Trust (the Trust) is the data controller for personal information processed by the Trust and its academies.

Registered/central office: Unit 5, Charnwood Edge Business Park, Cossington, Leicestershire, LE7 4UZ

Telephone: 0116 296 8171

Website: <https://www.aquinas-cmat.org>

Our Data Protection Officer (DPO) is Antoinette Bouwens. Questions about this notice or the way we use personal information can be sent to: dpo@aquinas-cmat.org or to the address above.

2. Who this notice applies to

This notice applies to members of the Trust workforce, including employees, workers, volunteers, trainee teachers, apprentices and individuals undertaking work experience or workplace placements. It applies to personal information processed in connection with recruitment, employment, engagement and the management of the working relationship.

3. The information we collect and use

Depending on your role and circumstances, we may process the following categories of information:

- personal and contact details, including name, address, telephone number, email address, date of birth, employee or teacher number and National Insurance number;
- emergency contact and next-of-kin details;
- characteristics and equality information, including age, sex, ethnicity, disability, religion or belief and other equality-monitoring information where collected;
- recruitment information, including applications, CVs, employment history, references, interview records and pre-employment checks;
- contract and employment information, including start and leaving dates, role, hours, FTE, place of work, salary and contractual terms;
- payroll, tax, expenses, bank and pension information;
- qualifications, professional registrations, training and continuing professional development records;
- attendance, leave and absence information, including sickness and family-related leave;
- performance management, appraisal, capability, grievance and disciplinary information;
- health, medical, occupational health, reasonable adjustment and workplace accident information where relevant;
- safeguarding and safer-recruitment information, including right-to-work checks, DBS information and information relating to criminal convictions or offences where the law permits us to process it;
- IT, communications, access-control, security and system-use information, and CCTV/images where applicable; and
- other information necessary to manage the employment or working relationship and meet our legal, regulatory and safeguarding responsibilities.

Some of this information is special category personal data and requires additional protection. Criminal offence information is also subject to additional legal safeguards.

4. Why we collect and use personal information

- recruit, appoint and onboard staff and other members of the workforce;
- administer contracts, pay, pensions, expenses, benefits, leave and attendance;

- manage and support the workforce, including performance, professional development, wellbeing, capability, grievance and disciplinary processes;
- meet safeguarding, safer-recruitment, health and safety and employment obligations;
- make appropriate workplace adjustments and manage occupational health referrals;
- monitor equality, diversity and workforce trends where lawful and appropriate;
- plan staffing, budgets, organisational development, recruitment and retention;
- protect Trust premises, systems, people and information;
- carry out internal audit, assurance, quality monitoring and investigations;
- complete statutory returns and provide information to public authorities where required; and
- establish, exercise or defend legal claims and obtain professional advice.

5. Our lawful bases

Under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018), we map each processing activity to its specific lawful basis and condition:

Purpose/Category of Data	Article 6 Lawful Basis (UK GDPR)	Article 9 Condition/DPA 2018 (Special Category & Criminal)
Recruitment, Onboarding & HR Management (CVs, references, contracts, role details)	Article 6(1)(b) Contract — Necessary to execute or enter into an employment contract.	N/A
Payroll, Pensions & Tax Administration (Bank details, NI number, tax codes)	Article 6(1)(c) Legal Obligation — Compliance with HMRC, statutory pay, and pension schemes.	N/A
Safeguarding & Criminal Checks (DBS disclosures, right-to-work)	Article 6(1)(c) Legal Obligation & Article 6(1)(e) Public Task — Keeping Children Safe in Education (KCSIE) regulations.	DPA 2018 Schedule 1, Part 1 & Part 2 (Employment, social security, and substantial public interest / safeguarding).
Sickness & Occupational Health (Medical notes, reasonable adjustments)	Article 6(1)(c) Legal Obligation — Statutory sick pay and workplace health and safety law.	Article 9(2)(b) (Employment and social security) & Article 9(2)(h) (Occupational medicine and assessment of working capacity).
Equality & Diversity Monitoring (Ethnicity, religion, disability checks)	Article 6(1)(c) Legal Obligation — Public Sector Equality Duty under Equality Act 2010.	Article 9(2)(g) & DPA 2018 Schedule 1, Part 2, Para 8 (Statutory and equality of opportunity monitoring).
Voluntary / Optional Activities (Staff profiles, optional photos/social media)	Article 6(1)(a) Consent — Where provided voluntarily.	Article 9(2)(a) Explicit Consent (if special category).

Clarification on Legitimate Interests (Article 6(1)(f)): As a public authority performing public tasks under Article 6(1)(e), the Trust does not rely on legitimate interests for core operational or statutory workforce functions. Legitimate interests are only relied upon for non-core, auxiliary activities such as securing IT network infrastructure or organizing staff wellbeing initiatives.

6. Special category and criminal offence information

Where we process special category personal data, we also identify an appropriate condition under Article 9 UK GDPR and, where required, a condition in the Data Protection Act 2018. Depending on the purpose, this may include employment, social security and social protection law; protecting vital interests in limited circumstances; occupational health; substantial public interest; legal claims; or another condition permitted by law.

Where we process criminal offence information, including information connected with DBS checks, we do so only where an appropriate lawful basis and a condition under the Data Protection Act 2018 apply, with appropriate safeguards.

7. How we collect information

We collect information directly from you through recruitment and application processes, forms, contracts, HR and payroll records, correspondence and systems used during your employment or engagement. We may also receive information from:

- previous employers and referees;
- recruitment agencies;
- the Disclosure and Barring Service;
- professional bodies and regulators;
- HM Revenue & Customs;
- pension providers;
- local authorities and the Department for Education;
- occupational health providers and health professionals; and
- other relevant public bodies or service providers.

Most of the information we require is necessary for contractual, statutory, safeguarding or operational reasons, but some is voluntary. We will make clear whether information must be provided and, where appropriate, the consequences of not providing it.

8. How long we keep information and how we protect it

We keep personal information only for as long as it is needed for the purpose for which it was collected, or for as long as we are required to keep it. Different records have different retention periods, which are set out in the Trust's Records Retention Schedule, available on the Trust SharePoint/Extranet or on request.

We use appropriate organisational and technical measures to protect personal information against accidental or unlawful loss, alteration, disclosure or access. Access is limited to people who need the information for their role. When information is no longer required, we dispose of it securely.

9. Who we share information with

We only share personal information where there is a lawful basis to do so. Depending on the circumstances, we may share information with:

- local authorities, where applicable;
- the Department for Education and other government departments or public authorities;
- HM Revenue & Customs;
- Teachers' Pensions and the Local Government Pension Scheme or relevant pension administrators;
- payroll, HR, IT, cloud, communications and other contracted service providers;

- occupational health and other health professionals;
- safeguarding bodies, the Disclosure and Barring Service, professional regulators and law-enforcement bodies where applicable;
- insurers, auditors, solicitors and other professional advisers;
- banks and financial service providers where necessary for payments;
- prospective employers or other organisations where we are lawfully providing a reference; and
- other organisations where we are required or permitted by law to disclose information.

Where an organisation processes personal data on our behalf, we put appropriate contractual and data protection arrangements in place. We do not rely on consent as the default basis for routine workforce data sharing.

10. Department for Education and School Workforce Census

The Department for Education (DfE) collects personal information from educational settings through statutory data collections, including the School Workforce Census. We are required to provide specified workforce information to the DfE where legislation requires this. The relevant census guidance identifies the legislation supporting each collection.

The DfE uses information collected from educational settings for purposes including funding, monitoring education policy and school accountability, statistics and research.

11. International transfers

Some suppliers or services may process or store personal information outside the United Kingdom. Where we transfer personal data internationally, we will do so in accordance with UK data protection law and will use an appropriate transfer mechanism and safeguards where required. You can ask our DPO for further information about relevant safeguards.

12. Consent and communications

Where we rely on consent for an optional use of personal information, we will explain what the information will be used for and how consent can be withdrawn. Withdrawing consent will not affect processing that took place lawfully before consent was withdrawn. Routine employment, safeguarding and statutory processing does not generally rely on consent.

13. Automated decision-making and profiling

We do not currently make decisions about members of the workforce that have legal or similarly significant effects based solely on automated processing. If this changes, we will provide appropriate privacy information explaining the processing, its significance and the rights available to individuals.

14. Your data protection rights

Depending on the circumstances and the lawful basis used, individuals may have the following rights under data protection law:

- the right to be informed about how personal information is used;
- the right of access to personal information;
- the right to have inaccurate information corrected;
- the right to erasure in certain circumstances;

- the right to restrict processing in certain circumstances;
- the right to data portability where it applies;
- the right to object to processing in certain circumstances;
- rights relating to automated decision-making and profiling; and
- the right to withdraw consent where consent is the lawful basis.

These rights are not absolute and do not all apply in every circumstance. To exercise a right, contact our DPO using the details in section 1.

15. Complaints

If you have a concern about our use of personal information, please contact our DPO first so that we can try to resolve it.

You also have the right to complain to the Information Commissioner's Office (ICO):

Website: <https://ico.org.uk/make-a-complaint/>

Telephone: 0303 123 1113

Post: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

16. Changes to this notice

We review this privacy notice at least annually and whenever there is a significant change to how we use personal information. The current version will be made available to the workforce through the Trust's usual communication channels.

17. Further information

For further information about data protection, to make a subject access request or to exercise another data protection right, contact the DPO using the details in section 1.