

Teacher and staff privacy notice

Updated September 2026 | Version 2.0 | England

This notice explains how we use personal information about current and former teachers and other staff, and applicants where relevant, why we need it, who we share it with and the rights you have. You do not need to sign or consent to this privacy notice. Optional publicity choices are provided separately at the end.

Who is responsible for your information

School: St Agnes CE Primary School. The data controller, which decides how and why personal information is used, is St Agnes Governing Body.

Controller contact: 50 Hamilton Road, Longsight, Manchester. M13 0PE. Where another organisation controls particular records, we explain its role when relevant.

Our Data Protection Officer service is provided by Global Policing Limited. Email: data@globalpolicing.co.uk. Telephone: 0161 510 2999 (answerphone). Website: www.globalpolicing.co.uk/data. You may contact the school or the DPO about this notice or your rights.

We follow the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, as amended, including by the Data (Use and Access) Act 2025.

Information we collect and where it comes from

We collect information from you, recruitment and supply agencies, referees, previous employers, qualification and vetting bodies, occupational health services, pension providers and relevant public authorities. We also create records while managing recruitment and employment. Information may include:

- Identity, contact and emergency-contact details; date of birth, National Insurance and teacher reference numbers; right-to-work and suitability checks.
- Applications, references, qualifications, experience, recruitment assessments and relevant publicly available professional information where lawfully checked.
- Contracts, role, pay, bank and pension details, tax, working hours, attendance, leave, performance, training, grievances and disciplinary records.
- Health and disability information, adjustments, ethnicity, religion and trade union information where needed and lawful; criminal record and safeguarding information subject to specific safeguards.
- Photographs, communications and workplace system records where relevant. Age and sex are not, by themselves, special category data under UK GDPR.

Why we use information and our lawful bases

We use information to recruit suitable staff, administer employment and pay, provide support and adjustments, manage performance and workplace issues, protect pupils and staff, meet statutory duties and maintain a reliable workforce record.

Recruitment employment and statutory duties

Contract under Article 6(1)(b) applies where processing is necessary to take steps you request before entering into a contract or to perform our employment contract, such as administering contractual pay and benefits.

Legal obligation under Article 6(1)(c) applies to relevant employment, tax, pension, right-to-work, equality, health and safety, safeguarding and statutory reporting duties. Where applicable, workforce returns are made under the Education (Supply of Information about the School Workforce) (No. 2) (England) Regulations 2007, as amended.

As a school (a public authority) (Public task under Article 6(1)(e)), our main legal basis for processing staff data (payroll, employment records, safeguarding checks) is that it is necessary to perform a task in the public interest—namely running a school and providing state education.

Sensitive and criminal record information

For special category information we also need an Article 9 condition. Necessary employment, social security and social protection processing, including relevant health and adjustment records, normally uses Article 9(2)(b) and Schedule 1 paragraph 1 of the Data Protection Act 2018. We keep an appropriate policy document where required.

Occupational health processing may use Article 9(2)(h) and Schedule 1 paragraph 2 where the required professional confidentiality safeguards apply. Necessary legal claims may use Article 9(2)(f). Safeguarding or equality monitoring may use Article 9(2)(g) with the appropriate Schedule 1 condition. Where we process special category data under Article 9(2)(g) and Schedule 1 of the Data Protection Act 2018 (such as safeguarding or equality monitoring), we maintain an Appropriate Policy Document (APD) setting out our procedures for securing compliance with the data protection principles and our policies regarding retention and erasure.

List of purposes:

1. Occupational Health & Medical Processing (Staff)
2. Safeguarding & Child Protection (Pupils & Staff)
3. Equal Opportunities & Diversity Monitoring (Pupils & Staff)
4. Legal Claims & Disputes (Staff, Parents, Visitors)

Criminal record and DBS information is subject to Article 10 and relevant domestic-law conditions. We limit access, record only what is necessary and apply specific retention rules.

To fulfill our statutory duties under Keeping Children Safe in Education (KCSIE) and employment law, the school processes criminal record data, including self-declarations and Disclosure and Barring Service (DBS) checks for staff, governors, and volunteers.

Lawful Conditions: We process this data under Article 10 UK GDPR in accordance with the following conditions under Schedule 1 of the Data Protection Act 2018:

- Paragraph 1: Employment, social security and social protection obligations.
- Paragraph 6: Statutory and government purposes.
- Paragraph 18: Safeguarding of children and individuals at risk.

Data Handling & Retention:

- We do not retain copies of DBS certificates for longer than 6 months following a recruitment decision, unless exceptional circumstances apply.

- We record only necessary confirmation details on our Single Central Record (SCR) (check date, certificate number, and verification outcome).
- Access to this data is restricted strictly to authorized senior leadership and HR staff. All processing is safeguarded under the school's Appropriate Policy Document (APD).

Choice and essential information

Optional publicity may use consent under Article 6(1)(a), with a genuine choice and no employment disadvantage for refusal. Consent is not the general basis for employment records or required checks. In an emergency vital interests may apply, subject to the additional conditions for sensitive information.

We tell you whether requested information is a legal or contractual requirement, necessary for a particular service or optional. Without essential information we may be unable to assess an application, confirm employment, pay you correctly or arrange a benefit or adjustment. Please keep your details up to date.

Sharing, protecting and retaining information

We share relevant information where necessary and lawful with payroll and pension administrators, HMRC, our local authority where applicable, the DfE, vetting and professional regulation bodies, occupational health providers, insurers, auditors, legal advisers and safeguarding or law-enforcement agencies. References are provided where appropriate and lawful.

1. Who We Share Workforce Data With

We share relevant staff personal data where necessary and lawful with the following categories of recipients:

- Financial & Administrative Bodies: HM Revenue & Customs (HMRC), statutory pension schemes (e.g., Teachers' Pensions, Local Government Pension Scheme - LGPS), and our contracted payroll provider (Local Authority Payroll).
- Local Authority: Manchester City Council for statutory returns, safeguarding duties, and financial reporting statutory duty as a maintained school.
- Department for Education (DfE): Under statutory data collections (e.g., the annual School Workforce Census under Sections 113 and 114 of the Education Act 2005).
- Regulatory & Vetting Bodies: The Disclosure and Barring Service (DBS), the Teaching Regulation Agency (TRA), Ofsted, and professional registration bodies.
- Health & Welfare Providers: Our occupational health service (Healthworks) and employee assistance scheme, Health Assured.
- Professional Services & Safety: Our insurers, legal advisers, internal/external auditors, and law enforcement or safeguarding agencies where required by law.
- Reference Enquiries: Prospective future employers, provided the request is lawful and appropriate.

We do not share workforce data with third parties for marketing purposes.

2. How We Protect Your Information

We maintain physical, technical, and organizational security measures to protect staff data against unauthorized access, loss, or misuse:

- Electronic systems (e.g., HR software, cloud storage) are password-protected with role-based access limits and multi-factor authentication.
- Physical records (e.g., paper personnel files, DBS checks) are kept in locked filing cabinets within restricted access areas.

- Third-party software providers handling staff data are vetted for UK GDPR compliance and process data under binding data processing agreements.

3. How Long We Retain Workforce Data

We hold workforce data securely in line with our Data Retention Policy, which is based on the IRMS (Information and Records Management Society) Toolkit for Schools:

- Main Personnel File: Retained for 2 years after the date employment ends.
- Payroll & Taxation Records: Retained for 6 years following the end of the financial year to which they relate (HMRC requirement).
- Unsuccessful Job Applications: Retained for 6 months post-interview, after which they are securely destroyed.
- Allegations / Safeguarding Involving Staff: Retained until normal retirement age or 10 years from the date of the allegation (whichever is longer), in accordance with statutory safeguarding guidance.
- DBS Clearance Records: Copies of certificates are destroyed within 6 months of inspection; basic verification data on the Single Central Record (SCR) is kept permanently.

4. Linked Policies and Further Information

For further details regarding how we manage personal data, please consult the following policies available on the school website or via the school office:

- Data Protection Policy: Website [link](#)
- Data Retention Policy & Schedule
- Appropriate Policy Document (APD) for Special Category Data
- DfE Privacy Notice Details: To learn more about how the Department for Education processes workforce data, visit GOV.UK Workforce Privacy Notice.

Suppliers supporting HR, payroll, IT, training and school management systems may process information for us under written instructions and contractual safeguards. Other recipients act as independent controllers. Our DPO may access information needed to advise us or help manage a request or complaint. Details of service providers: School Business Manager.

Where required, we supply workforce information for statutory returns to the DfE, directly or through the local authority (Manchester City Council). The DfE uses workforce information for education workforce statistics, analysis and policy. Its privacy information explains its own use and sharing: <https://www.gov.uk/government/publications/privacy-information-education-providers-workforce-including-teachers>.

Workforce categories:

- Teachers: Qualified and unqualified teachers, leadership staff (Headteacher and Deputy/Assistant Headteachers).
- Support Staff: Teaching assistants, higher level teaching assistants (HLTAs), pastoral, special educational needs (SEN) support staff, learning mentors, and educational welfare officers.
- School Business & Administrative Staff: School Business Managers/Bursars, HR, finance, administrative, ICT, and clerical support roles.
- Site & Specialist Staff: Premises managers, caretakers, catering staff, and cleaning or maintenance personnel directly employed by the school.

Security and monitoring

We restrict access to those who need information for their role and apply appropriate security, confidentiality and staff training measures. Health, employment casework, vetting and safeguarding information have access controls appropriate to their sensitivity.

Security and Monitoring

1. Access Controls and Security Measures

We restrict access to personal data strictly to staff members who require it to perform their official duties. We apply appropriate technical, physical, and organisational security, confidentiality, and staff training measures:

- **Special Category & Sensitive Data:** Health records, employment casework files, vetting details, and safeguarding records are subject to strict role-based access controls and encrypted storage appropriate to their high sensitivity.
- **IT & Cybersecurity Support:** We partner with a contracted third-party IT service provider, MGL Ltd, who assist and support the school with our system infrastructure, cybersecurity management, technical monitoring, and device security. MGL Ltd process system data strictly under a binding UK GDPR-compliant data processing agreement.

2. System Monitoring, Filtering, and Logging

To maintain network security, protect school property, and fulfill our statutory safeguarding duties under Keeping Children Safe in Education (KCSIE), we operate the following technical monitoring systems:

- **Internet Filtering & Web Security:** All web traffic on school devices and networks is filtered to prevent access to illegal, harmful, or inappropriate content. MGL Ltd support the management of these filtering controls.
- **Data Collected:** IP addresses, device identifiers, domain requests, timestamps, and flagged content search terms.

Purpose & Lawful Basis: Safeguarding pupils and staff; network security.

- **Safeguarding pupils and staff:** Protecting the physical, emotional, and digital safety/wellbeing of students and employees (e.g., monitoring online activity for harmful content or self-harm risks).
- **Network security:** Maintaining the stability, performance, and cyber-defense of institutional networks, devices, and systems.

Lawful Basis:

- Data processing is necessary for performing a task carried out in the public interest or in the exercise of official authority vested in the controller (common for state schools, academies, and public institutions).
- Processing is necessary to comply with a statutory legal requirement (such as statutory safeguarding duties under education law).

Email & Device Logs: System logs of network activity, email metadata (sender, recipient, timestamp), and software usage are automatically generated and reviewed where security breaches, safeguarding concerns, or policy violations occur.

Purpose: System security, prevention of cyber threats, statutory duty of care. The specific, explicit, and legitimate reasons for processing personal data (e.g., monitoring network traffic, log analysis, firewall filtering, endpoint monitoring)

Lawful Basis: 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.

Retention: Monitoring logs are securely stored and retained for in accordance with our Retention Policy, after which they are automatically overwritten or deleted unless required for an ongoing investigation.

3. Physical Access, CCTV, and Other Systems

Closed-Circuit Television (CCTV): We operate CCTV on school premises for premises security, crime prevention, and staff/pupil safety. Signage is prominently displayed at entry points. CCTV footage is retained for 30 days before automatic deletion.

Building Access Control: Staff electronic door passes log entry to secure school areas for safety and site security. Entry logs are accessed only by authorised site management.

Biometric Systems: We do not collect or process biometric data (such as fingerprint readers or facial recognition) for staff or pupils.

Automated Decision-Making & AI Tools: We do not use AI-supported automated tools or algorithms for staff recruitment, candidate shortlisting, or HR performance evaluations. All recruitment and HR decisions are conducted directly by human decision-makers.

4. Further Information

For full details regarding IT usage, acceptable use conditions, and network security policies, please consult the school's Acceptable Use Policy and Safeguarding Policy (contact the Office for copies).

International transfers: Personal information is accessed outside the UK, including through cloud providers. This is carried out only with prospective candidates from any country. Appropriate security and safeguarding data is requested from relevant authorities. Data is held in accordance with the section – 'Sharing, protecting and retaining information'.

How long we keep information

We retain information only as long as needed for its purpose, taking account of legal duties, pension administration, safeguarding and legal claims. We apply separate periods to recruitment, employment, payroll, tax, pension, health, safeguarding, monitoring and consent records. Our retention schedule is available on our Data Retention policy (request copies from the Office).

We do not apply a single two-year or five-year limit to all staff records. Some records need shorter retention and others substantially longer. Relevant safeguarding allegation records are generally retained until normal pension age or for ten years from the allegation, whichever is later, subject to applicable guidance and exceptions. Pension and statutory financial records have their own requirements.

Where a complaint, investigation, legal claim or preservation requirement justifies continued retention, we keep the relevant records for the necessary period and review that need. When no longer required, information is securely destroyed or anonymised. We explain particular retention arrangements if you ask.

Your rights and how to contact us

You can ask for access to your personal information and correction of inaccurate or incomplete information. Depending on the lawful basis and circumstances, you may also ask for erasure, restriction of use or a portable copy, or object to processing. These rights have conditions and exceptions; for example, we may need to retain records to meet a legal duty.

Where we rely on consent, you can withdraw it at any time without affecting the lawfulness of earlier use. Where we rely on public task or legitimate interests, you may object on grounds relating to your circumstances. You can object to direct marketing at any time.

Contact the school or our DPO to exercise your rights. Requests can be made verbally or in writing and do not have to use a particular form. We may need proportionate evidence of identity or authority to protect your information. We normally respond to a subject access request within one calendar month. Where the law allows clarification, an extension or an exemption, we will explain how this affects your request. School holidays do not automatically extend the deadline.

Automated decisions

We do not make any decisions about current staff members, governors, volunteers, or prospective job applicants based solely on automated processing (including profiling) that produces legal effects or significantly affects an individual.

All key decisions regarding employment, recruitment shortlisting, performance management, disciplinary procedures, and pay progression are conducted directly by human decision-makers (such as interview panels, senior leadership, line managers, and governing boards).

Should the school ever introduce automated decision-making tools in the future, this privacy notice will be updated prior to implementation, and affected individuals will be provided with full details regarding the underlying logic, likely consequences, and their right to request human intervention and contest decisions under Article 22 of the UK GDPR.

Questions and complaints

If you are concerned about our use of personal information, contact the school or Global Policing Limited using the details on the first page. Our data protection complaints procedure is available by clicking [here](#). We will acknowledge a data protection complaint within 30 days, investigate appropriately, keep you informed and provide an outcome without undue delay.

You also have the right to complain to the Information Commissioner's Office (ICO). Visit <https://ico.org.uk/make-a-complaint/> or call 0303 123 1113. The ICO normally expects you to give the organisation an opportunity to address your concern first.

Keeping this notice up to date

We review this notice regularly and when our use of information changes. We will bring material changes to your attention. Current notice: <https://www.st-agnes.manchester.sch.uk/page/privacy-notice/147025>

Next scheduled review: September 2027, or sooner if needed. Ask the school for an accessible format or help understanding this notice.

Optional photographs and publicity consent

School: St Agnes CE Primary School. This form records optional choices only. Refusing or withdrawing consent will not affect your employment, opportunities or treatment at work.

Staff member name: _____

Select Yes or No for each purpose. Leaving a choice blank means no consent for that purpose. Photographs may include video images. We will seek a separate choice for any materially different use. This form does not authorise facial recognition or biometric identification.

Use images in optional celebration displays inside the school, without a name. Yes ☐ No ☐

Add my name to those internal celebration displays. Yes ☐ No ☐

Publish images on the school's public website, without a name. Yes ☐ No ☐

Add my name to those website images. Yes ☐ No ☐

Publish images on the school's official social media accounts, without a name. Yes ☐ No ☐

Add my name to those social media images. Yes ☐ No ☐

Use images in printed school prospectuses or publicity leaflets, without a name. Yes ☐ No ☐

There are no official social media accounts covered. Online publication and printed-stock retention: School Website and Prospectus. We will ask separately before providing identifiable images or names to newspapers or other external publishers.

Public images can be viewed, copied or shared by others, including outside the UK. We control our own publications but cannot guarantee removal of copies made by others. To withdraw or change a choice, contact admin@st-agnes.manchester.sch.uk or call 0161 224 6829. We will stop future consent-based use and remove images from channels we control where reasonably possible; already distributed printed material may not be recoverable.

These choices are voluntary. Permission to publish my name applies only where permission for the associated image has also been given. Necessary identification and employment records are covered by the privacy notice and do not depend on this form.

Signature: _____ Date: _____

We retain evidence of your choices and any withdrawal in accordance with our retention schedule, for as long as necessary to manage and demonstrate those choices.