



Holy trinity staff and workforce Privacy Notice

Academic Year 2026 and 2027

Headteacher / Data Protection Lead	Mrs Jade Wakefield
DPO service	Staffordshire County Council
Effective from	September 2026
Review date	September 2027
Version	1.0

Document control

Document title	Staff and Workforce Privacy Notice
School	Holy Trinity Church of England (Controlled) Primary School
Document owner	Headteacher
Headteacher / Data Protection Lead	Mrs Jade Wakefield
DPO service	Staffordshire County Council
Approval	Governing Board / appropriate governing body
Review cycle	At least annually and whenever there is a significant change to processing

Status note. This notice is designed for publication and staff circulation. It should be checked against the school's live systems, contracts, retention schedule and governance arrangements before formal approval.

1. Purpose and scope

Holy Trinity Church of England (Controlled) Primary School ("the school", "we", "us" or "our") is committed to protecting the privacy, confidentiality and security of personal information relating to its workforce.

This notice explains what personal information we collect, why we use it, the lawful bases on which we rely, who we may share it with, how long we keep it, how we protect it and the rights available to individuals.

It applies, as relevant, to current and former employees, teachers, support staff, senior leaders, casual and temporary workers, agency workers, contractors, consultants, apprentices, volunteers, trainee teachers, students on placement and applicants for roles at the school.

This notice should be read alongside the school's Data Protection and Privacy Policy, Records Retention Schedule, Safeguarding and Child Protection Policy, Staff Code of Conduct, Acceptable Use / IT policies, CCTV information and other relevant HR and information-governance procedures.

2. Data controller and key contacts

For the processing described in this notice, Holy Trinity Church of England (Controlled) Primary School acts as a data controller where it determines the purposes and means of processing personal data, subject to any controller arrangements that apply through the school's governance structure.

Headteacher / Data Protection Lead: Mrs Jade Wakefield

School address: Wetmore Road, Burton upon Trent, DE14 1SN

Telephone: 01283 247550

Email: office@holytrinity.staffs.sch.uk

The school's Data Protection Officer service is provided by Staffordshire County Council.

DPO email: dpo.schools@staffordshire.gov.uk

The DPO provides independent advice and oversight on data protection compliance and acts as a point of contact for data protection matters.

3. Data protection framework

We process personal data in accordance with applicable UK data protection law, including the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and relevant amendments made by the Data (Use and Access) Act 2025, together with applicable education, employment, safeguarding and records-management requirements.

We apply the data protection principles. Personal data must be processed lawfully, fairly and transparently; collected for specified and legitimate purposes; adequate, relevant and limited to what is necessary; accurate and kept up to date; retained no longer than necessary; and protected by appropriate security. We are also responsible for demonstrating compliance with these principles.

4. Personal information we collect

Identity and contact information: name; title; previous names; date of birth; address; telephone numbers; personal and work email addresses; emergency contacts; next of kin; photographs; employee/personnel identifiers.

Recruitment and vetting information: application forms; CVs; employment history; references; interview notes and assessments; qualifications; professional registrations; identity and right-to-work evidence; DBS and barred-list information; prohibition or restriction checks; safer-recruitment records.

Employment and contractual information: job title; department; employment status; contract; start and leaving dates; working pattern; hours; continuous service; probation; flexible-working arrangements; secondments; role changes; contractual correspondence.

Pay, pension and financial information: salary; allowances; expenses; benefits; bank details; tax information; National Insurance number; pension information; statutory payments; deductions; payroll records.

Attendance and leave information: working hours; annual leave; sickness absence; family-related leave; special leave; time off and related records.

Performance and professional information: appraisals; objectives; professional development; training; capability; disciplinary and grievance information; complaints; investigations; professional correspondence.

Safeguarding and suitability information: safeguarding concerns or allegations; referrals; suitability checks; information relevant to working with children; criminal-offence information where processing is authorised by law.

Health, equality and wellbeing information: health information; medical conditions; disability and reasonable adjustments; occupational-health information; accident information; equality-monitoring data where collected lawfully.

IT, communications and security information: usernames; account identifiers; authentication and login records; device and network information; school-system activity; internet and email metadata; filtering and monitoring alerts; printing records; access-control information; security logs; CCTV images and other recordings where applicable.

5. Special category and criminal-offence data

Some workforce information receives additional protection under data protection law. This may include information about health, disability, racial or ethnic origin, religious or philosophical beliefs, trade union membership, sexual orientation, sex life, genetic data and biometric data used for unique identification.

Where we process special category data, we identify both an Article 6 lawful basis and an appropriate Article 9 condition. Depending on the circumstances, relevant conditions may include employment and social-protection obligations and rights, substantial public interest, occupational medicine and assessment of working capacity, vital interests, legal claims, or other conditions authorised by law.

Criminal-conviction and offence data, including DBS and barred-list information, is processed only where we have an appropriate lawful basis and legal authority or a condition under the Data Protection Act 2018. This is particularly relevant to safeguarding, safer recruitment and suitability to work with children.

Where required by law, the school maintains an Appropriate Policy Document covering relevant special category and criminal-offence processing.

6. How we obtain personal information

Most workforce information is provided directly by the individual, for example during recruitment and throughout employment or engagement. We may also receive information from:

- previous employers and referees
- recruitment or supply agencies
- Staffordshire County Council and other public authorities
- the Department for Education (DfE) and Teaching Regulation Agency
- the Disclosure and Barring Service
- professional or regulatory bodies
- HM Revenue & Customs and pension providers
- occupational-health or healthcare providers
- safeguarding agencies, police, courts and tribunals
- our IT, security, access-control, CCTV, filtering and monitoring systems
- service providers acting on our behalf
- publicly accessible sources where lawful and necessary

7. Why we use workforce information

- recruiting, selecting and appointing staff and other workers;
- carrying out safer-recruitment, identity, qualification and right-to-work checks;
- performing employment and other contracts;
- paying salaries, expenses and benefits and administering tax, National Insurance and pensions;
- workforce planning, management, reporting and statutory returns;
- managing attendance, absence, leave, health, safety and wellbeing;
- considering and implementing reasonable adjustments;
- managing appraisal, performance, training and professional development;
- managing disciplinary, capability, grievance and complaint processes;

- meeting safeguarding and child-protection duties and maintaining required safer-recruitment records;
- meeting education, employment, equality, health and safety, tax, pension and other legal obligations;
- protecting pupils, staff, visitors, premises, systems and confidential information;
- operating and securing IT, communications, filtering and monitoring systems;
- preventing, detecting and investigating misuse, fraud, security incidents and cyber threats;
- responding to audits, inspections, legal claims, court proceedings and regulatory enquiries;
- providing employment references where appropriate;
- managing emergencies and business continuity; and
- supporting the effective governance and operation of the school.

8. Lawful bases for processing

The school does not rely on one lawful basis for all workforce processing. The basis depends on the particular purpose and circumstances.

UK GDPR basis	When it may apply	Examples
Article 6(1)(b) – Contract	Necessary for a contract with you or steps requested before entering one.	Employment administration, contractual pay and benefits.
Article 6(1)(c) – Legal obligation	Necessary to comply with a legal obligation.	Tax, pensions, employment law, safer recruitment, safeguarding and statutory reporting.
Article 6(1)(e) – Public task	Necessary for a task in the public interest or exercise of official authority, where applicable.	Delivery and administration of public education functions and related statutory duties.
Article 6(1)(d) – Vital interests	Necessary to protect someone’s life.	Exceptional emergencies.
Article 6(1)(f) – Legitimate interests	Used where legally available, necessary and balanced against individual rights.	Certain security, administration or organisational purposes where appropriate.
Article 6(1)(a) – Consent	Used only where consent is genuinely appropriate and freely given.	Limited optional uses where another basis does not apply.

Because of the imbalance that can exist in an employment relationship, consent will not normally be the preferred basis where another lawful basis is available. Where consent is relied upon, it can be withdrawn without affecting processing that was lawful before withdrawal.

9. Sharing workforce information

We share personal information only where there is a lawful reason and only to the extent necessary. Depending on the circumstances, recipients may include:

- Department for Education
- Staffordshire County Council
- other schools, academies or trusts where lawful
- HM Revenue & Customs
- Teachers’ Pension Scheme, Local Government Pension Scheme and relevant pension administrators
- payroll, HR and occupational-health providers
- Disclosure and Barring Service

- Teaching Regulation Agency and other professional regulators
- Ofsted and other inspection or regulatory bodies
- safeguarding partners and relevant local safeguarding arrangements
- police, courts, tribunals and other law-enforcement bodies
- insurers, auditors and professional advisers
- IT, MIS, cloud, communications, cyber-security, filtering and monitoring providers
- recruitment, training, wellbeing and employee-assistance providers
- trade unions or representatives where authorised or otherwise lawful

Where a supplier processes personal data on our behalf, we use appropriate contractual and security arrangements. We may also disclose information where required by law, for safeguarding, to protect vital interests, to prevent or detect crime, or to establish, exercise or defend legal claims.

10. Department for Education and workforce data

The school is required to provide certain workforce information to the Department for Education, directly or through the local authority where applicable. This includes statutory workforce data collections such as the School Workforce Census.

The DfE processes education workforce information for functions including education policy, workforce planning, research, statistics, funding, monitoring and accountability. The DfE publishes its own privacy information for the education workforce. Consent is not required where the school is legally required or otherwise authorised to provide the information.

11. IT, filtering, monitoring and communications

Use of school devices, networks, accounts and systems may generate information that is logged, filtered, monitored or reviewed. Purposes may include safeguarding pupils, cyber security, preventing unauthorised access or malware, investigating suspected misuse, protecting confidential information, maintaining system availability and complying with legal or regulatory obligations.

Any worker monitoring must be lawful, fair, transparent, necessary and proportionate. The school will identify the purpose and lawful basis, limit collection to what is necessary, restrict access and consider whether a Data Protection Impact Assessment (DPIA) is required. Workers will normally be informed about monitoring. Covert monitoring would only be considered in exceptional circumstances and subject to appropriate authorisation and safeguards.

Detailed operational arrangements should be read alongside the school's Acceptable Use, Online Safety, Filtering and Monitoring and Information Security arrangements, including the systems monitored, who can access alerts or reports and applicable retention periods.

12. CCTV and other recordings

Where CCTV or other recording systems are operated, they may capture images of staff and other individuals. Such systems will be used only for specified and lawful purposes, which may include safeguarding, site security, protection of people and property, health and safety, and prevention or investigation of crime or serious incidents.

Access to recordings will be restricted to authorised persons. Recordings will be retained only for the period justified by the purpose, unless they need to be preserved for an investigation, safeguarding matter or legal proceedings. Appropriate signage and additional privacy information will be provided where required.

13. Artificial intelligence and automated decision-making

The school may use digital tools that incorporate artificial intelligence or automated functionality. Before introducing processing that is likely to create a high risk to individuals, the school will consider and, where required, complete a DPIA and implement appropriate safeguards.

The school will not treat the use of an AI system as removing human responsibility for decisions. Where solely automated decision-making produces legal effects or similarly significant effects and the relevant legal provisions apply, individuals will be given the information and safeguards required by data protection law.

14. International transfers

Some technology or service providers may process or store personal data outside the United Kingdom. Where a restricted international transfer takes place, the school will ensure that an appropriate lawful transfer mechanism and safeguards are in place, such as UK adequacy regulations, the UK International Data Transfer Agreement, the UK Addendum to the EU Standard Contractual Clauses, or another permitted mechanism.

Further information about relevant safeguards can be requested from the school or DPO.

15. Retention and disposal

We do not keep personal data for longer than necessary. Retention periods vary according to the type of record, the purpose for which it is held, and legal, safeguarding, pension, contractual, operational or evidential requirements.

The school's Records Retention Schedule / Records Management arrangements set out the applicable periods. At the end of the relevant period, information will be securely deleted, destroyed or anonymised unless there is a lawful reason to retain it for longer.

The UK GDPR does not prescribe a single retention period for workforce records. The school therefore documents and periodically reviews its retention decisions.

16. Information security

We use appropriate technical and organisational measures to protect personal information from accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access. Measures may include access controls, authentication, encryption where appropriate, backups, secure configuration, staff training, supplier due diligence, secure disposal and incident-management procedures.

Access to workforce information is restricted according to role and business need. Staff must comply with school policies governing confidentiality, information security and acceptable use.

17. Data breaches

The school maintains procedures for identifying, reporting, assessing, managing and recording personal-data breaches. Staff must report suspected or actual breaches promptly in accordance with school procedures.

Where a breach is likely to result in a risk to individuals' rights and freedoms, the school will notify the Information Commissioner's Office where required. Where a breach is likely to result in a high risk, affected individuals will also be informed where required by law.

18. Your data protection rights

Right to be informed: to receive clear information about how personal data is used.

Right of access: to request a copy of personal data held about you, subject to applicable exemptions.

Right to rectification: to ask for inaccurate data to be corrected and incomplete data completed.

Right to erasure: to ask for deletion in circumstances where the right applies; it is not an absolute right.

Right to restriction: to request restriction of processing in certain circumstances.

Right to data portability: to receive certain data in a structured, commonly used and machine-readable format where the statutory conditions apply.

Right to object: to object to certain processing, including some processing based on public task or legitimate interests.

Rights relating to automated decision-making: to receive applicable safeguards where relevant solely automated decisions have legal or similarly significant effects.

The availability of a particular right depends on the circumstances and the lawful basis for processing. To exercise a right, contact the school or the DPO. We may need to verify identity before responding.

19. Accuracy of your information

Please tell the school promptly if information we hold about you changes or is inaccurate. This includes changes to your name, address, contact details, emergency contacts, bank details, qualifications or other information the school reasonably needs to keep accurate.

20. Complaints and concerns

If you have a concern about how the school has handled your personal information, please contact the Headteacher / Data Protection Lead or the DPO in the first instance.

Headteacher / Data Protection Lead: Mrs Jade Wakefield, Holy Trinity CE (C) Primary School, Wetmore Road, Burton upon Trent, DE14 1SN. Telephone: 01283 247550. Email: office@holytrinity.staffs.sch.uk.

Data Protection Officer service: Staffordshire County Council. Email: dpo.schools@staffordshire.gov.uk.

You also have the right to raise a concern with the Information Commissioner's Office (ICO), the UK's independent data protection regulator. ICO: Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. Telephone: 0303 123 1113. Website: ico.org.uk.

21. Changes to this notice

This notice will be reviewed at least annually and whenever there is a significant change to the way workforce personal data is processed. Where a change materially affects individuals, the school will take appropriate steps to bring the change to their attention.

Effective from: September 2026

Next scheduled review: September 2027

22. Related school documents

- Data Protection and Privacy Policy
- Records Retention Schedule / Records Management Policy
- Personal Data Breach Procedure
- Information Security / Cyber Security arrangements
- Acceptable Use Policy
- Online Safety and Filtering & Monitoring arrangements
- CCTV Policy / privacy information, where applicable
- Safeguarding and Child Protection Policy
- Staff Code of Conduct
- Recruitment and Selection / Safer Recruitment procedures
- HR policies and procedures
- Subject Access Request procedure
- Artificial Intelligence guidance or policy, where applicable

23. Sources and statutory guidance used

This notice has been prepared with reference to the following current guidance and sources. These sources should be checked when the notice is reviewed because data protection guidance can change.

- Department for Education, Privacy notice model documents for schools and local authorities (updated 13 August 2026).
- Department for Education, Issuing privacy notices: guidance for schools and local authorities (updated 13 August 2026).
- Department for Education, Data protection in schools: data protection policies and procedures.
- Department for Education, Privacy information: education providers' workforce, including teachers (updated 7 September 2026).
- Information Commissioner's Office, Employment information guidance, including Data protection and monitoring workers.
- Holy Trinity CE (C) Primary School, Data Protection and Privacy Policy (January 2026) and published GDPR information.