EAST CLAYDON C of E SCHOOL & PRESCHOOL

Data Protection Policy

2026–2027

School information	Details
School	East Claydon Church of England School
Policy owner	Headteacher
Data Protection Officer	Nicola Cook
Approved by	Governing Board
Date approved	September 2026
Review date	September 2027

'BUILDING EACH OTHER UP'

1. Statement of intent

East Claydon C of E School & Preschool is required to keep and process certain information about pupils, parents and carers, staff, volunteers, governors, visitors, contractors and other individuals in accordance with data protection legislation. The school is committed to protecting personal data, using it lawfully, fairly and transparently, and ensuring that information is handled securely and proportionately.

This policy sets out how the school meets its responsibilities under the UK GDPR, the Data Protection Act 2018 and related legislation. It also reflects updated Department for Education guidance for schools, including the Data Use and Access Act 2025, cyber security and safeguarding considerations, filtering and monitoring, the use of photos, videos and CCTV, and generative artificial intelligence in education.

All staff, governors, volunteers and adults working on behalf of the school must understand that protecting personal data is part of safeguarding, professional conduct and public trust.

2. Legal and statutory framework

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Data (Use and Access) Act 2025
- Freedom of Information Act 2000
- Protection of Freedoms Act 2012
- Privacy and Electronic Communications Regulations 2003
- Education (Pupil Information) (England) Regulations 2005, as amended
- School Standards and Framework Act 1998
- Keeping Children Safe in Education 2025 and the published 2026 guidance, where applicable
- Working Together to Safeguard Children
- DfE Data protection in schools guidance, updated 9 July 2026
- DfE Generative AI: product safety standards, updated 19 January 2026
- ICO guidance for schools, universities and colleges

This policy should be read alongside the school's Child Protection and Safeguarding Policy, Online Safety Policy, Acceptable Use Policy, CCTV Policy, Freedom of Information Policy, Freedom of Information Publication Scheme, Records Management Policy, Staff Code of Conduct, Data Breach Procedure and any relevant privacy notices.

3. Key definitions

Area	Expectation
Personal data	Any information relating to an identified or identifiable living individual. This includes names, contact details, identification numbers, location data, online identifiers and information that can identify someone when combined with other data.
Special category data	More sensitive personal data requiring additional protection, including data about health, biometric data used for identification, racial or ethnic origin, religious or philosophical beliefs, trade union membership, genetic

	data, and data concerning sex life or sexual orientation.
Criminal offence data	Personal data relating to criminal convictions, offences, allegations, proceedings or related security measures. This includes DBS information.
Data controller	The organisation that decides why and how personal data is processed. The school is the data controller for much of the personal data it processes.
Data processor	An organisation or person that processes personal data on behalf of the school, such as a supplier providing a management information system, safeguarding system, communication platform or cloud service.
Personal data breach	A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. Data protection principles

The school will ensure that personal data is:

- processed lawfully, fairly and transparently
- collected for specified, explicit and legitimate purposes
- adequate, relevant and limited to what is necessary
- accurate and kept up to date where necessary
- kept in a form that permits identification for no longer than necessary
- processed securely using appropriate technical and organisational measures
- managed in a way that enables the school to demonstrate compliance

The school will promote data minimisation and privacy by design when introducing new systems, forms, processes, apps, platforms, AI tools or information-sharing arrangements.

5. Roles and responsibilities

5.1 Governing Board

- Ensure appropriate data protection policies, procedures and privacy notices are in place.
- Receive assurance that data protection risks are identified and managed.
- Ensure the school has access to independent DPO advice.
- Support a culture where personal data is protected and used responsibly.

5.2 Headteacher

- Ensure this policy is implemented in day-to-day practice.
- Ensure staff are trained and know how to report concerns or breaches.
- Ensure new systems or significant processing changes are discussed with the DPO.
- Ensure data protection is considered alongside safeguarding, SEND, HR, finance, governance and operational decisions.

5.3 Data Protection Officer

- Inform and advise the school about data protection obligations.
- Monitor compliance and provide advice on DPIAs, privacy notices and processing arrangements.

- Advise on data breaches and information rights requests.
- Act as a contact point for the ICO and for individuals whose data is processed.

East Claydon's Data Protection Officer is Nicola Cook. Queries and data requests should be directed to the school office or the DPO contact details held by the school. The DPO contact details should be checked before publication of this policy.

5.4 Staff, governors and volunteers

- Handle personal data only where there is a legitimate school purpose.
- Use school-approved systems and follow security expectations.
- Do not disclose personal data unless authorised and secure.
- Report suspected data breaches immediately.
- Seek advice from the Headteacher, School Business Manager or DPO where unsure.

6. Lawful processing and privacy notices

The school will identify and document the lawful basis before processing personal data. The most common bases in school are legal obligation, public task, contract, vital interests, consent and, in limited circumstances, legitimate interests.

Special category and criminal offence data will only be processed where a UK GDPR Article 9 or Article 10 condition and relevant Data Protection Act 2018 Schedule 1 condition apply. This includes safeguarding, employment, health, SEND, equality, statutory education duties and legal claims where relevant.

Privacy notices will be clear, accessible and age-appropriate where needed. They will explain what data is collected, why it is used, the lawful basis, how long it is retained, who it is shared with, rights available to individuals and how to complain.

- pupils and families
- prospective pupils and families
- school workforce
- governors and trustees
- volunteers
- suppliers, contractors and visitors

7. Information rights requests

Individuals, including children where they have sufficient understanding, have rights in relation to personal data held by the school. These include the right to be informed, access, rectification, erasure, restriction, objection, data portability in limited circumstances, and rights relating to automated decision-making.

Subject access requests and other information rights requests may be made verbally or in writing. Staff receiving a request must pass it promptly to the Headteacher, School Business Manager or DPO. The school will verify identity before releasing information and will consider whether disclosure would reveal another person's personal data or cause serious harm.

The school will respond without undue delay and within one month unless an extension is lawfully available because the request is complex or numerous. Where a request is manifestly unfounded or excessive, the school may refuse the request or charge a reasonable fee, in line with data protection law.

8. Records of processing, data mapping and retention

The school will maintain appropriate records of processing activities, especially where processing is not occasional, presents risk to individuals, involves special category data or criminal offence data, or uses third-party systems.

- the purpose of processing
- categories of individuals and personal data
- lawful basis and special category condition where required
- recipients or categories of recipients
- retention period or retention criteria
- technical and organisational security measures
- processor arrangements, contracts and data sharing agreements
- international transfer arrangements where applicable

The school will retain records only for as long as necessary and in line with the school's Records Management Policy and retention schedule. Record retention should be reviewed when systems, statutory duties or local arrangements change.

9. Data protection by design and DPIAs

Data protection will be considered at the start of any new project, procurement, digital system, monitoring activity, AI tool, data-sharing arrangement or substantial change in processing. The school will complete a Data Protection Impact Assessment where processing is likely to result in high risk to individuals.

- new or significantly changed MIS, safeguarding, behaviour, communication, assessment or monitoring systems
- AI-enabled tools or automated decision-making features
- large-scale processing of special category data
- CCTV, biometric systems or monitoring technologies
- filtering and monitoring systems that process pupil or staff data
- new EdTech products or suppliers processing personal data

Where a DPIA identifies a high risk that cannot be mitigated, the school will consult the ICO before starting the processing.

10. Data sharing and safeguarding

The UK GDPR does not prevent or limit the sharing of information for the purposes of keeping children safe. Staff must not allow fears about data protection to obstruct safeguarding action. Where information is needed to identify, assess or respond to risk, staff must share it with appropriate people or agencies in a timely and proportionate way.

Where information is shared for safeguarding, the school will record what was shared, with whom, why it was shared, whether consent was sought, and where consent was not sought, the reason. Safeguarding information must be shared and recorded in line with the Child Protection and Safeguarding Policy.

The school may also share personal data with the local authority, DfE, health services, social care, police, courts, Ofsted, professional advisers, insurers, auditors, payroll providers, pension providers, educational platforms and other schools where lawful and necessary.

11. Data security

- Paper records containing personal data must be stored securely and not left unattended or visible to unauthorised people.
- Electronic records must be held on approved systems with secure access controls.
- School devices must be password protected and secured when not in use.
- Personal devices should not be used for school data unless specifically authorised and secured.
- Sensitive or confidential emails must be checked carefully before sending and protected where appropriate.
- Bulk emails to parents and carers must use approved systems or blind carbon copy where necessary.
- USB sticks and removable media must not be used for personal data unless authorised, encrypted and necessary.
- Personal data taken off site must be protected from loss, theft or unauthorised access.
- Visitors must not have access to confidential or personal information.

The school will review technical and organisational measures regularly and will seek DPO, IT or specialist advice where significant risks are identified.

12. Cyber security, filtering and monitoring

The school recognises that cyber security, online safety, filtering and monitoring can involve the processing of personal data. These systems must be lawful, proportionate, transparent and aligned with safeguarding responsibilities.

- Filtering and monitoring systems should be documented and subject to review.
- Where monitoring records alerts, user activity or other identifiable data, the privacy notice must explain this clearly.
- Access to monitoring data must be limited to authorised staff with a legitimate need.
- AI-supported or automated monitoring tools must be assessed for accuracy, fairness, proportionality and risk.
- Filtering and monitoring concerns will be managed in line with online safety and safeguarding procedures.

13. Photos, videos and CCTV

Images and video recordings of identifiable individuals are personal data and must be handled in line with data protection principles. The school will be clear about why images are taken, how they are used, how long they are retained and who they may be shared with.

Consent will be sought where required, for example for promotional use of pupil images. Consent must be specific, informed and capable of being withdrawn. Where images are used for safeguarding, security, education or statutory purposes, another lawful basis may apply.

CCTV will only be used where necessary and proportionate. Signs or notices will inform pupils, staff and visitors about CCTV use. Footage will be stored securely, accessed only by authorised people and retained in line with the CCTV Policy and retention schedule.

The school will remind parents and visitors that images taken for personal and domestic purposes should not be published or shared in a way that includes other children without appropriate permission.

14. Cloud services, EdTech and suppliers

Before using cloud services, EdTech products or digital platforms that process personal data, the school will consider data protection risks, security arrangements, supplier responsibilities, retention and deletion arrangements, access controls, data location and whether a contract or data processing agreement is required.

- confirm whether the supplier acts as controller, processor or joint controller
- ensure contracts include appropriate data protection clauses
- check whether pupil data may be used for analytics, product development or AI model training
- ensure privacy information is clear for pupils, parents and staff
- ensure access is removed when staff leave or no longer require access
- review supplier arrangements when systems change or contracts are renewed

15. Generative artificial intelligence and automated decision-making

Generative AI tools must be used cautiously and only in line with school policy, safeguarding expectations, data protection law and professional judgement. Staff and pupils must not enter personal, identifiable, confidential or sensitive data into generative AI tools unless the tool has been approved by the school following appropriate risk assessment and, where required, a DPIA.

AI tools must not be used to make solely automated decisions with legal or similarly significant effects for pupils, parents, staff or governors. This includes decisions about admissions, grading, behaviour sanctions, attendance intervention, SEND provision, safeguarding, recruitment, appraisal or disciplinary matters. Human oversight is required.

- assess the stated purpose and educational use case of any AI product
- consider security, privacy, data retention and data minimisation
- consider age, SEND, safeguarding, equality and bias risks
- avoid relying solely on AI-generated outputs
- report AI-related concerns, suspected breaches or unsafe outputs promptly

16. Personal data breaches

All suspected data breaches must be reported immediately to the Headteacher, School Business Manager or DPO. A breach may include sending information to the wrong recipient, losing a device or paper record, unauthorised access, accidental deletion, cyber attack, inappropriate disclosure, or use of an unapproved system.

The DPO will support the school to assess whether a personal data breach has occurred, what risk it presents, what action is needed, whether the ICO must be notified within 72 hours, and whether affected individuals must be informed. The school will keep a record of breaches, decisions and actions taken.

The school will use breach learning to reduce future risk, including refresher training, changes to systems, staff guidance, access controls or procedures where appropriate.

17. DBS and recruitment data

DBS and safer recruitment data will be handled securely and only by authorised staff. DBS information will not be copied or retained beyond what is necessary and lawful. Any third party handling DBS or recruitment information must understand their data protection responsibilities.

18. Training and awareness

All staff will receive data protection information as part of induction and ongoing training. Training will include personal data handling, safeguarding information sharing, cyber security, information rights requests, data breaches, AI and use of approved systems. Governors and volunteers will receive information appropriate to their role.

19. Compliance with this policy

All employees, governors, volunteers, agency staff, contractors and any other adults working on behalf of East Claydon Church of England School are expected to comply with this policy. This includes handling personal data securely, using approved systems, following privacy and retention requirements, reporting data breaches promptly and seeking advice where unsure.

Any failure to comply with this policy, including unauthorised disclosure, misuse of personal data, failure to report a suspected breach, inappropriate use of AI or digital systems, or failure to follow data protection procedures, may be treated as a disciplinary matter and managed through the school's disciplinary procedures.

Where non-compliance contributes to safeguarding concerns, breaches of statutory duty or risks to individuals, the school may also need to consult or refer matters to relevant external agencies, the ICO or professional bodies where appropriate.

20. Monitoring and review

This policy will be reviewed annually by the Headteacher and Governing Board, and sooner if statutory guidance changes, DfE or ICO guidance changes, the school introduces significant new processing, or a data incident identifies a need for review.

Next scheduled review: September 2027.