



Data Protection Policy

2026-27

Policy owner	Headteacher
Approval body	Full Governing Body
Data controller	Toynton All Saints Primary School
Data Protection Officer	Wayne Oldfield
Date approved	October 2026
Next review due	September 2027

1. Purpose and scope

Toynton All Saints Primary School is committed to protecting the personal data of pupils, parents and carers, staff, governors, volunteers, visitors and other individuals. This policy sets out how the school collects, uses, stores, shares, retains and securely disposes of personal data and how it responds when individuals exercise their information rights.

The policy applies to personal data in any format and to all staff, governors, volunteers, contractors and other people processing personal data on behalf of the school. Failure to follow this policy may result in disciplinary, contractual or other appropriate action.

2. Legal and regulatory framework

- UK General Data Protection Regulation (UK GDPR);
- Data Protection Act 2018;
- Data (Use and Access) Act 2025;
- Privacy and Electronic Communications Regulations 2003, where applicable;
- Education (Pupil Information) (England) Regulations 2005;
- Protection of Freedoms Act 2012, where biometric data is used; and
- other education, safeguarding, employment, equality and records-management law relevant to the processing.

The school will have regard to current guidance from the Information Commissioner's Office and the Department for Education, including guidance on data protection in schools, generative artificial intelligence, photography, video and CCTV.

3. Definitions

Term	Meaning
Personal data	Information relating to an identified or identifiable living person.
Special category data	More sensitive information, including data about health, racial or ethnic origin, religion or belief, trade-union membership, genetics, biometrics used for identification, sex life or sexual orientation.
Criminal offence data	Personal data about criminal convictions, offences, allegations, proceedings or related security measures.
Processing	Any operation performed on personal data, including collection, recording, organisation, storage, use, sharing, alteration, retrieval, anonymisation, erasure or destruction.
Data subject	The individual to whom personal data relates.
Controller	The organisation that determines why and how personal data is processed.

Term	Meaning
Processor	An organisation or person processing personal data on behalf of a controller, other than the controller's employee.
Personal data breach	A security breach leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. Controller, governance and accountability

Toynton All Saints Primary School is the data controller for the personal data for which it determines the purposes and means of processing. The school will maintain its required registration and fee arrangements with the ICO.

Governing Body

- has overall responsibility for ensuring compliance and effective governance;
- approves this policy and receives appropriate assurance from the DPO and school leaders;
- ensures sufficient resources, training and oversight; and
- does not seek access to identifiable personal data unless this is necessary and lawful for its functions.

Data Protection Officer

- operates independently and reports to the highest management level;
- monitors compliance, provides advice and supports training and audits;
- advises on data protection impact assessments;
- is the contact point for data subjects and the ICO; and
- reports significant risks and recommendations to the Governing Body.

Headteacher

The Headteacher represents the controller on a day-to-day basis, ensures procedures are followed, supports the DPO and ensures that staff understand their responsibilities.

All staff and governors

- process personal data only as required for authorised duties;
- keep data accurate, confidential and secure;
- use approved systems, devices and suppliers;
- complete required training;
- seek advice before starting new or changed high-risk processing;
- recognise and immediately report information-rights requests and data protection complaints; and
- report any actual or suspected personal data breach without delay.

5. Data protection principles

- lawfulness, fairness and transparency;
- purpose limitation;
- data minimisation;
- accuracy;
- storage limitation;
- integrity and confidentiality; and

- accountability for demonstrating compliance.

6. Lawful processing

Before processing personal data, the school will identify and document an appropriate lawful basis. The most commonly used bases are legal obligation, public task, contract, vital interests, legitimate interests where the public-authority restriction does not apply, and consent where consent is genuinely optional and can be withdrawn.

Special category and criminal offence data require an additional condition in law and, where required, an appropriate policy document. The school will not assume that consent is needed simply because information is sensitive. Consent will not be bundled with unrelated matters or relied upon if there is a clear imbalance of power and another lawful basis is more appropriate.

7. Fairness, transparency and privacy notices

- provide clear privacy information when data is collected, or within the applicable period when obtained elsewhere;
- explain the controller and DPO contacts, purposes, lawful bases, recipients, retention, transfers, rights and complaint route;
- review privacy notices when processing changes;
- communicate in language appropriate to children and the intended audience; and
- carry out a compatibility assessment or provide updated information before using data for a materially different purpose.

8. Records, minimisation, accuracy and retention

- maintain records of processing activities and an information asset register;
- collect only data that is adequate, relevant and necessary;
- provide routes for individuals to correct inaccurate data;
- apply an approved records retention schedule;
- place retention holds on records needed for a complaint, request, safeguarding matter, investigation or legal claim; and
- securely delete, anonymise or destroy data when retention ends.

9. Sharing and disclosures

Personal data will be shared only where there is a lawful basis, the sharing is necessary and proportionate, and appropriate safeguards are in place. Consent is not always required, including where the school must share to meet a legal duty, perform a public task, protect vital interests or safeguard a child.

- verify the identity and authority of the recipient;
- share the minimum necessary information securely;
- record significant or non-routine disclosures;
- use data sharing agreements where appropriate;
- consult the DPO for unusual, systematic or high-risk sharing; and
- follow current safeguarding information-sharing guidance.

Processors, suppliers and educational technology

Before appointing a processor or digital service, the school will complete proportionate due diligence and ensure a written contract contains the required data-protection terms. The school will identify whether each supplier is acting as processor, independent controller or joint controller; review sub-processors, security, retention, deletion and international transfers; and complete a DPIA where high risk is likely.

10. International transfers

Personal data will not be transferred outside the UK unless the transfer is lawful and appropriate safeguards are in place. The school will seek DPO advice, document the transfer mechanism and consider supplementary measures where required.

11. Information rights and requests

Individuals may have rights to be informed, access personal data, rectification, erasure, restriction, objection, data portability and safeguards relating to automated decision-making. Rights are not absolute and will be considered under the applicable law.

Subject access requests

- Requests may be verbal or written and must be forwarded immediately to the DPO or designated school contact.
- The school may request proportionate information to confirm identity and clarify the scope where necessary.
- The school will normally respond without undue delay and within one month, subject to lawful extension for complex or numerous requests.
- Information will normally be supplied free of charge; a reasonable fee or refusal may apply to manifestly unfounded or excessive requests.
- Third-party information and other exempt material will be carefully considered and redacted or withheld where the law requires or permits.

Children and parental requests

A child's personal data belongs to the child. Whether a parent or carer may exercise a child's information rights will depend on the child's competence and the circumstances. This is separate from the statutory parental right to access the educational record of a pupil at a maintained school. Requests to inspect the educational record will be handled within 15 school days; a lawful copying fee may apply.

Automated decision-making

Where solely automated processing produces legal or similarly significant effects, the school will identify a lawful basis and provide applicable safeguards, including clear information, an opportunity to make representations, challenge the decision and obtain human intervention. Special category data will receive the additional protection required by law.

12. Data protection complaints

The school will provide an accessible route for people to make a data protection complaint. A complaint may be made to the school office, Headteacher or DPO and may be verbal or written. The school will:

- acknowledge the complaint within 30 days of receipt;
- take appropriate steps without undue delay, including making necessary enquiries;
- keep the complainant appropriately informed;
- communicate the outcome without undue delay;
- keep a record of the complaint, investigation, decision and action; and
- explain the right to complain to the ICO if the individual remains dissatisfied.

13. Security and acceptable handling

- apply role-based access and remove access promptly when roles change;
- use strong authentication, approved password controls and multi-factor authentication where available;
- encrypt school laptops, portable devices and removable media containing personal data;
- use approved school accounts and systems rather than personal messaging, email or storage;
- keep paper records and devices secure and clear desks and screens when unattended;

- use secure methods for sharing sensitive information and check recipients before sending;
- not leave personal data unattended in vehicles;
- report phishing, malware, loss, misdirection or unauthorised access immediately; and
- follow the school's cyber-security, acceptable-use, home-working and business-continuity procedures.

14. Data protection by design and DPIAs

Privacy will be considered at the start of any project, system, process or significant change. A DPIA must be completed before high-risk processing begins, including certain uses of new technology, large-scale special category data, systematic monitoring, biometrics, CCTV, profiling, artificial intelligence or innovative educational technology. The DPO will advise and any unmitigated high risk will be handled in accordance with the law.

15. Artificial intelligence

- Only AI tools approved by the school may be used for school business.
- Staff must not enter identifiable, confidential, safeguarding, special category or criminal offence data into an AI tool unless the use has been specifically approved following appropriate due diligence and, where required, a DPIA.
- Personal accounts must not be used to process school personal data.
- Outputs affecting individuals must be checked by a competent person; significant decisions will not be delegated to an AI tool without lawful safeguards and meaningful human oversight.
- The school will be transparent about relevant AI processing and will review supplier terms, data reuse, model training, retention, deletion, age appropriateness, security and international transfers.
- Suspected unauthorised disclosure to an AI service must be reported as a potential personal data breach.

16. Photographs, video and audio

The school will identify a lawful basis for taking and using images and recordings and explain the purpose. Consent will be used for optional promotional uses where appropriate and may be withdrawn for future use. Images will be stored securely, retained only as necessary and shared only through approved channels. Safeguarding considerations may require additional restrictions even where data-protection law does not apply to a family's purely personal use.

17. CCTV and surveillance

If CCTV is used, the school will document its necessity, proportionality, purposes, lawful basis, coverage, access, retention and disclosure arrangements. Clear signage will identify the controller and purpose. CCTV will not be used in places where individuals reasonably expect privacy; audio recording will require separate justification and advice. Access will be restricted and disclosures recorded.

18. Biometric data

The school does not introduce an automated biometric recognition system without Governing Body approval, DPO advice, a DPIA and compliance with the Protection of Freedoms Act 2012. Written parental consent and the child's rights will be respected, and a suitable alternative will be provided for pupils who do not participate.

19. Personal data breaches

Any person who becomes aware of an actual or suspected breach must immediately notify the DPO or the school's designated reporting contact. Staff must not investigate independently beyond urgent containment or delete relevant evidence.

- contain the incident and secure systems, records and accounts;
- preserve evidence and establish what happened, whose data is involved and the likely consequences;
- assess risk to individuals;

- record the facts, effects, decisions and remedial action for every breach;
- notify the ICO without undue delay and, where feasible, within 72 hours of awareness where the breach is likely to risk individuals' rights and freedoms;
- inform affected individuals without undue delay where a high risk is likely, unless an exception applies; and
- review lessons, controls and training.

20. Training, monitoring and audit

- all staff and governors receive induction and refresher training appropriate to their role;
- specialist training is provided for staff handling high-risk data or requests;
- completion is recorded and non-completion followed up;
- the DPO may carry out audits, spot checks and reviews; and
- the Governing Body receives proportionate assurance on risks, breaches, requests, complaints, DPIAs, training and improvement actions.

21. Review and related documents

This policy will be reviewed at least annually and sooner when legislation, guidance, technology, processing or organisational arrangements change. The DPO will advise on review and the Full Governing Body will approve the policy.

- Privacy notices and records of processing activities
- Retention and disposal schedule
- Data breach procedure and register
- Subject access and information-rights procedure
- Data protection complaints procedure
- Freedom of Information publication scheme
- Safeguarding and Child Protection Policy
- Online Safety and Acceptable Use Policy
- CCTV policy, where applicable
- Photography and image-use arrangements
- AI policy or acceptable-use guidance
- Cyber-security and business-continuity procedures

Appendix 1: Immediate breach response

Step	Required action	Owner / record
1. Report	Notify the DPO/designated contact immediately. Give facts, not assumptions.	
2. Contain	Recall email where possible, disable links/accounts, recover devices or records, and prevent further disclosure without destroying evidence.	
3. Assess	Identify data, people affected, sensitivity, volume, security protections and potential harm.	

Step	Required action	Owner / record
4. Decide	DPO records the risk assessment and decision on ICO and individual notification.	
5. Notify	Make required notifications within applicable timescales and keep information clear and factual.	
6. Learn	Record actions, address causes, update controls and training, and monitor completion.	

Approval record

Date approved: October 2026 Chair of Governors: Corinna Wright Headteacher: Neil Mitchell