Data Protection Policy

Last updated September 2026

Approved by the Board of Trustees

Next scheduled review September 2027

Contents

Statement of intent
1. Legal framework
2. Scope and applicable data
3. Data protection principles and accountability
4. Roles and responsibilities
5. Lawful processing
6. Consent
7. Transparency and privacy information
8. Right of access
9. Right to rectification
10. Right to erasure
11. Right to restrict processing
12. Right to data portability
13. Right to object
14. Information rights requests
15. Data protection complaints
16. Automated decision making and profiling
17. Data protection by design and default
18. Data Protection Impact Assessments
19. Data sharing and safeguarding
20. Personal data breaches
21. Information security
22. Generative AI and educational technology
23. Publication of information
24. CCTV photography and recordings
25. Cloud services and international transfers
26. Records management and retention
27. DBS and criminal offence data
28. Training assurance and audit
29. Monitoring and review
Appendix 1 Personal data breach response
Appendix 2 Information rights request workflow

Statement of intent

Tyne and Wear Learning Trust and its academies must collect and use personal information about pupils, families, staff, volunteers, governors, trustees, contractors and other members of the school community. The trust will do so lawfully, fairly, transparently and securely, and will protect the rights and freedoms of every person whose information it holds.

This policy explains the trust-wide arrangements for compliance with the UK GDPR, the Data Protection Act 2018 and the Data (Use and Access) Act 2025. It applies to information held electronically and on paper, and to all processing carried out on behalf of the trust, including by suppliers, cloud services and artificial intelligence systems.

Data protection supports, and does not prevent, effective safeguarding. Personal information will be shared promptly where this is necessary and proportionate to protect a child or another person from harm. Staff must not allow uncertainty about data protection to delay a safeguarding referral.

All staff, governors, trustees, volunteers and contractors who handle personal information must follow this policy, complete required training, use approved systems and report suspected breaches immediately.

1. Legal framework

This policy has due regard to relevant legislation and statutory guidance, including:

- UK General Data Protection Regulation, as amended by the Data (Use and Access) Act 2025
- Data Protection Act 2018, as amended
- Data (Use and Access) Act 2025 and its commencement regulations
- Freedom of Information Act 2000 and Environmental Information Regulations 2004
- Privacy and Electronic Communications (EC Directive) Regulations 2003, as amended
- Education (Pupil Information) (England) Regulations 2005, as amended
- Protection of Freedoms Act 2012 and the Surveillance Camera Code of Practice
- Human Rights Act 1998 and Equality Act 2010
- Children Act 1989 and Children Act 2004
- Keeping Children Safe in Education 2026
- Working Together to Safeguard Children 2026
- DfE Data protection in schools guidance, updated July 2026
- ICO UK GDPR guidance, Children's code, right of access guidance and data protection complaints guidance
- DfE Generative artificial intelligence in education guidance and applicable cyber security standards.

This policy should be read with the trust's Freedom of Information, Records Management and Retention, Cyber Security, Acceptable Use, CCTV, Photography and Images, Child Protection and Safeguarding, Staff Privacy, Pupil Privacy and Data Breach procedures.

2. Scope and applicable data

Personal data is information relating to an identified or identifiable living person. It includes names, identifiers, contact details, online identifiers, location data, opinions, images, recordings and information that can identify a person when combined with other data. Pseudonymised information remains personal data where re-identification is possible. Information that has been irreversibly anonymised is not personal data.

Special category data includes information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, and genetic, biometric, health, sex-life or sexual-

orientation data. Criminal offence data includes allegations, proceedings, convictions and related security measures. These categories require an additional condition and stronger safeguards.

The policy covers automated processing and structured paper records. It also covers personal data entered into, generated by or inferred through digital platforms, monitoring tools, biometric systems, learning analytics and generative AI services.

3. Data protection principles and accountability

The trust will ensure that personal data is:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes and not used incompatibly;
- adequate, relevant and limited to what is necessary;
- accurate and kept up to date where necessary;
- kept in identifiable form only for as long as required;
- protected by appropriate technical and organisational measures; and
- processed in a way the trust can evidence through records, policies, training and assurance.

The trust will maintain a record of processing activities, data asset and information flow records, privacy notices, lawful-basis assessments, contracts, retention schedules, breach records, information-rights logs and DPIAs. Each academy must cooperate with trust-wide assurance and promptly report changes to systems, suppliers or processing.

4. Roles and responsibilities

Board of Trustees

The Board of Trustees is accountable for ensuring that the trust has appropriate governance, resources and assurance for data protection and information security. It will receive proportionate reports on significant risks, breaches, complaints and improvement actions.

Executive leaders and headteachers

Executive leaders and headteachers will implement this policy, ensure staff training, provide adequate systems and controls, support the DPO's independence, and ensure that local processing and procurement are authorised and documented.

Data Protection Officer

The DPO will inform and advise the trust, monitor compliance, advise on DPIAs, provide a contact point for data subjects and the ICO, and report independently to the highest management level. The DPO will have timely access to information, resources and decision-makers and will not be instructed on how to perform the role.

All staff and authorised users

All users must process personal data only for authorised purposes, follow security requirements, use approved devices and services, apply retention rules, recognise information-rights requests, and report incidents immediately. Deliberate or reckless misuse may result in disciplinary action and referral to relevant authorities.

Processors and suppliers

Processors may act only on documented instructions. Contracts must address confidentiality, security, sub-processors, assistance with rights and breaches, deletion or return, audit and international transfers. The trust remains responsible for selecting and monitoring processors.

5. Lawful processing

Before processing begins, the trust will identify and record a lawful basis under Article 6 UK GDPR. The bases most commonly used by schools and trusts are legal obligation and public task. Contract, vital interests, consent and legitimate interests may apply where their conditions are met. Public authorities must not rely on legitimate interests when performing their public tasks.

Where special category data is processed, the trust will identify an Article 9 condition and, where required, a condition in Schedule 1 to the Data Protection Act 2018 and an appropriate policy document. Criminal offence data will be processed only under official authority or where authorised by law with suitable safeguards.

The Data (Use and Access) Act 2025 introduced recognised legitimate interests for specified purposes and clarified some compatible further processing. Any reliance on these provisions must be documented and approved by the DPO. They do not remove the need for necessity, proportionality, fairness, transparency or compliance with other legal duties.

When another public authority requests data to perform a public task or official function, the requesting authority is responsible for identifying why the disclosure is necessary for that function. The trust must still verify the request, establish its own lawful basis for disclosure, share only what is necessary and keep a record.

6. Consent

Consent will be used only where a genuine choice exists and the trust can demonstrate that it is freely given, specific, informed and unambiguous. It must be as easy to withdraw consent as to give it. Refusal or withdrawal must not create detriment where consent is the lawful basis.

Consent will not normally be used for core education, employment, safeguarding or statutory functions because of the imbalance of power or the availability of another lawful basis. Separate consent may be appropriate for optional photographs, publicity or non-essential communications.

For an information society service offered directly to a child, the trust will apply the UK age of digital consent and verify parental authorisation where required. The child's competence, best interests and evolving capacity will be considered in all decisions concerning their rights.

7. Transparency and privacy information

Privacy notices will be concise, transparent, intelligible and accessible, using clear language suitable for the audience, particularly children. They will explain the controller and DPO, purposes, lawful bases, categories, recipients, retention, international transfers, rights, complaints and relevant automated decision making.

Notices will be reviewed when processing changes. Where information is obtained indirectly, the trust will provide privacy information within the statutory period unless an exemption applies. Any disproportionate-effort exception for research or archiving will be documented and accompanied by appropriate safeguards and publicly available information.

8. Right of access

A subject access request may be made verbally or in writing, including through social media, and does not need to mention data protection law. Staff must forward any request immediately to the DPO or designated information-rights lead. The trust will respond without undue delay and normally within one month.

The response period begins when the trust receives the request, or when necessary identity or authority evidence, or an authorised fee, is received. It may be extended by up to two further months for complex or numerous requests, with reasons given within the first month.

The trust may seek clarification only where reasonably required. The response clock pauses from the day clarification is requested and resumes the day after it is received. The trust will make a reasonable and proportionate search, as clarified by the Data (Use and Access) Act 2025, and will document search decisions.

Information about another person will be disclosed only with consent or where it is reasonable to do so. Relevant exemptions, including those for education, social work, child abuse, legal privilege, management information and exam material, will be considered case by case. Information will be supplied securely and in a clear, accessible format.

9. Right to rectification

Individuals may ask the trust to correct inaccurate personal data or complete incomplete data. The trust will investigate and respond within one month, subject to any lawful extension. Where appropriate, processing will be restricted during verification. Recipients will be informed of corrections unless this is impossible or involves disproportionate effort.

10. Right to erasure

Individuals may request erasure where data is no longer necessary, consent has been withdrawn, an objection succeeds, processing is unlawful or erasure is legally required. The right is not absolute and may not apply where processing is necessary for legal obligations, public tasks, freedom of expression, public health, archiving or legal claims. Decisions and any refusal will be recorded and explained.

11. Right to restrict processing

The trust will restrict processing where accuracy is contested, processing is unlawful and restriction is preferred to erasure, data is needed for legal claims, or an objection is being assessed. Restricted data will normally be stored but not otherwise used without consent or another permitted reason. Recipients will be notified where required.

12. Right to data portability

Where processing is based on consent or contract and carried out by automated means, individuals may receive data they provided in a structured, commonly used and machine-readable format and may ask for direct transmission where technically feasible. This right does not apply to processing necessary for the trust's public tasks.

13. Right to object

Individuals may object to processing based on public task or legitimate interests. The trust will stop unless it demonstrates compelling legitimate grounds that override the person's interests, rights and freedoms, or the processing is needed for legal claims. Objections to direct marketing will always be honoured. Privacy notices will draw attention to this right clearly and separately.

14. Information rights requests

The DPO or information-rights lead will maintain a central log and coordinate searches, redaction, exemptions, approvals and secure disclosure. Identity checks must be necessary and proportionate. Requests from representatives require evidence of authority. Requests concerning children will be

decided according to the child's competence, wishes, best interests, welfare and privacy, rather than parental responsibility alone.

A reasonable fee may be charged only where permitted, including for manifestly unfounded or excessive requests or further copies. A high threshold applies. Any refusal must explain the reasons and the right to complain to the trust, the ICO and the courts.

15. Data protection complaints

The trust will provide an accessible way to complain about its use of personal data, including an electronic route. It will acknowledge a complaint within 30 days, take appropriate steps to investigate and respond without undue delay, keep the complainant informed, and communicate the outcome without undue delay.

Complaints will be logged and handled impartially. The outcome will explain any remedial action and the right to complain to the ICO. Complaint themes will inform training, risk management and policy improvement. The complaints route does not prevent a person from contacting the ICO at any time.

16. Automated decision making and profiling

The trust will identify any decision based solely on automated processing that produces legal or similarly significant effects. Following the Data (Use and Access) Act 2025, a wider range of lawful bases may be available for such decisions, but safeguards remain mandatory. The trust will provide meaningful information about the logic and consequences, enable representations, and provide human intervention and a route to contest the decision.

Stricter rules apply where special category data is used. No significant decision about a pupil or staff member will be delegated to an automated system without prior approval, a DPIA, verified lawful basis, bias and accuracy testing, appropriate human oversight and a clear appeal route.

17. Data protection by design and default

Privacy will be built into projects, procurement and operational change from the outset. Default settings will limit collection, access, use, retention and disclosure to what is necessary. Measures may include minimisation, pseudonymisation, encryption, role-based access, multi-factor authentication, logging, secure configuration, testing and documented review.

Where an online service is likely to be accessed by children, the trust will explicitly consider children's higher protection needs, best interests, age and understanding. The ICO Children's code and DfE guidance will be applied where relevant.

18. Data Protection Impact Assessments

A DPIA must be completed before processing likely to result in high risk, including systematic monitoring, large-scale special category data, biometrics, innovative technology, significant automated decisions, online services for children, or combining datasets in unexpected ways. The DPO will advise on the need, scope and adequacy of the assessment.

The DPIA will describe the processing, assess necessity and proportionality, identify risks to people, and record mitigations, owners and review dates. Processing must not begin until residual high risks are reduced to an acceptable level or the ICO has been consulted where required.

19. Data sharing and safeguarding

Personal data may be shared where there is a lawful basis and the disclosure is necessary, proportionate and secure. Routine sharing will be covered by privacy information, contracts or data-sharing agreements. One-off disclosures will be recorded with the requester, purpose, lawful basis, information shared and authorisation.

Safeguarding information will be shared in accordance with Keeping Children Safe in Education 2026, Working Together to Safeguard Children 2026 and current DfE information-sharing advice. Consent is not required where there is another lawful basis. The child's safety and welfare are paramount, and relevant information must be shared promptly with the DSL, children's social care, police or other appropriate agencies when needed to protect a child.

Staff must share the minimum information necessary, distinguish fact from opinion, verify recipients and use secure methods. Where appropriate and safe, individuals will be told about sharing. Reasons for sharing or not sharing will be documented.

20. Personal data breaches

A personal data breach includes accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. Examples include misdirected email, lost devices, inappropriate access, cyberattack, accidental publication and insecure disposal.

All suspected breaches must be reported immediately through the trust's incident route. Staff must preserve evidence, limit further disclosure and must not investigate or notify affected people independently. The DPO will coordinate containment, recovery, risk assessment and documentation.

Where a breach is likely to risk people's rights and freedoms, the trust will notify the ICO without undue delay and, where feasible, within 72 hours of awareness. Where the risk is high, affected people will also be informed without undue delay unless an exception applies. Every breach and decision will be recorded, whether or not notification is required.

21. Information security

The trust will apply controls proportionate to risk and current recognised standards. These will include:

- approved devices, accounts and systems with role-based least-privilege access;
- strong authentication and multi-factor authentication where appropriate;
- supported software, prompt security updates, malware protection and secure configuration;
- encryption in transit and at rest where proportionate, with managed backups and tested recovery;
- filtering, monitoring and logging consistent with safeguarding and privacy requirements;
- clear-desk, secure printing, locked storage and verified confidential disposal;
- secure remote working and restrictions on removable media and personal devices;
- supplier due diligence, contractual controls and ongoing service review;
- regular testing, incident exercises and improvement tracking.

Users must verify recipients before sending, use blind copy for group emails where addresses should not be disclosed, avoid personal accounts and unapproved applications, lock screens when unattended, and report phishing or suspicious activity. Personal data must not be transferred to private devices or consumer AI services without express authorisation.

22. Generative AI and educational technology

Only approved AI and EdTech services may process trust information. Before adoption, the trust will establish controller and processor roles, lawful basis, transparency, security, retention, data location,

sub-processors, model-training use, age suitability, accessibility and exit arrangements. A DPIA will be completed where high risk is likely.

Staff and pupils must not enter personal, special category, confidential, safeguarding, assessment or commercially sensitive information into an AI service unless the use has been specifically approved and protected. AI outputs may be inaccurate, biased or reveal personal data and must be checked by a competent person. Significant decisions must retain meaningful human oversight.

Contracts and settings should prevent supplier reuse for model training where possible, minimise telemetry, restrict retention and provide deletion and audit rights. The trust will maintain an approved-service register and review material changes to service terms or models.

23. Publication of information

Before publishing names, images, results, work or other personal data, the trust will identify a lawful basis, provide appropriate privacy information, minimise the data and consider foreseeable risks. Optional publicity will normally use consent. Statutory publication duties and legitimate school communications will be handled under the appropriate lawful basis.

Information published online may be copied, indexed and retained by others. Staff must use approved channels and remove information when it is no longer required. Complaints or objections will be considered promptly.

24. CCTV photography and recordings

CCTV and other surveillance will be used only for specified and proportionate purposes. Signage and privacy information will explain its use. Access, disclosure, retention and deletion will be controlled, and new or materially changed systems will be assessed through a DPIA.

Photographs, video and audio will be captured and used only for authorised purposes. Personal devices must not be used unless an approved exception applies. Images used for safeguarding, behaviour or evidential purposes will be managed as records and not reused for publicity without a separate lawful basis.

25. Cloud services and international transfers

Cloud and hosted services require procurement approval, security and privacy due diligence, a compliant data-processing contract, clear responsibilities, resilience arrangements and an exit plan. The trust will know where data is stored and which sub-processors are used.

Personal data may be transferred outside the UK only where a valid mechanism applies, such as UK adequacy regulations, the UK International Data Transfer Agreement or UK Addendum, together with any required transfer risk assessment and supplementary measures. The Data (Use and Access) Act 2025 amendments to the transfer test will be applied in line with current ICO guidance.

26. Records management and retention

Records will be accurate, findable, secure and retained in accordance with the trust's retention schedule, legal duties, limitation periods, safeguarding requirements and operational need. Retention periods will be documented by record category and reviewed regularly. Legal holds, investigations, complaints and active claims suspend routine deletion where relevant.

At the end of the retention period, records will be securely deleted, anonymised or transferred for archiving where justified. Paper records will be confidentially destroyed and digital media securely erased or destroyed. Disposal will be documented for significant record sets.

27. DBS and criminal offence data

DBS and other criminal offence information will be processed only where authorised by law and subject to Schedule 1 Data Protection Act 2018 conditions and the trust's appropriate policy document. Access will be strictly limited. Certificates will not normally be copied or retained beyond what is permitted; required check details will be recorded on the single central record.

Information received through the DBS Update Service will be handled in accordance with the DBS code of practice, employment law and safer recruitment requirements. Unauthorised disclosure may be a criminal offence and may result in disciplinary action.

28. Training assurance and audit

All staff will complete data protection and information security training at induction and refresher training at least annually. Role-specific training will be provided for leaders, governors, trustees, the DPO, DSLs, HR, IT, records staff and those handling information-rights requests or procurement.

Compliance will be monitored through audits, breach and complaint analysis, access reviews, supplier assurance, DPIA review, retention checks, cyber testing and reports to senior leaders and trustees. Actions will have named owners and completion dates. Serious or repeated non-compliance will be escalated.

29. Monitoring and review

The DPO will monitor legal and regulatory developments and advise on interim changes. Senior management will review this policy at least annually, after any significant incident, or sooner where legislation, statutory guidance, ICO guidance, technology or trust operations materially change.

The next scheduled review date is September 2027. The Board of Trustees must approve material amendments. Current approved versions will be communicated to staff and made available to relevant members of the school community.

Appendix 1 Personal data breach response

Stage	Required action	Owner
1 Report	Notify the designated incident route immediately. Preserve evidence and do not contact affected people unless instructed.	Person discovering incident
2 Contain	Stop further loss or disclosure, recall messages where possible, secure accounts or devices, and preserve logs.	IT or operational lead
3 Assess	Confirm data, people, circumstances, likely consequences, safeguards and recovery; determine when the trust became aware.	DPO with relevant leads
4 Decide	Record whether ICO notification is required and whether affected people must be informed.	DPO and controller decision-maker
5 Notify	Where required, notify the ICO within 72 hours of awareness and affected people without undue delay.	DPO or authorised lead
6 Recover	Restore services and data, support affected people, preserve evidence and manage safeguarding or disciplinary issues.	Incident team
7 Review	Record lessons, controls, owners and deadlines; report significant matters to senior leaders and trustees.	DPO and senior management

Appendix 2 Information rights request workflow

1. Recognise and forward the request immediately, including verbal and social-media requests.
2. Log the request and confirm the applicable right, scope and statutory deadline.
3. Request only necessary and proportionate identity, authority or clarification information.
4. Preserve potentially relevant records and issue search instructions to appropriate custodians and systems.
5. Carry out and document a reasonable and proportionate search.
6. Review for accuracy, third-party information, exemptions, safeguarding risk and legal restrictions.
7. Obtain DPO or authorised approval and disclose securely in a clear and accessible format.
8. Record the response, searches, redactions, exemptions, delivery method and any follow-up complaint.