



Data Protection Policy

Author:	Leona Bateman – Director of Data Strategy & Information Systems
Date:	1 September 2026
Audience:	All staff



Index

1. Purpose and scope	3
2. Legal Framework	3
3. Data protection principles	3
4. Data Governance and accountability	4
5. Roles and responsibilities	4
6. Lawful basis and special category data	5
7. Transparency and privacy notices	6
8. Children's data and safeguarding	6
9. Information rights	6
10. Data sharing, processors and suppliers	7
11. Records management, retentions and disposal	7
12. DPIA's and privacy by design	7
13. Biometrics, photos, videos and CCTV	8
14. Artificial Intelligence and Automated Decision-Making	8
15. Information Security and Cloud Computing	9
16. Data breaches and incident management	9
17. Training monitoring and assurance	9
18. Related policies	10
19. Review and approval	10

Appendices

Appendix A – Glossary of Terms	11
Appendix B – Trust Governance Terms	14
Appendix C - Information Sheet: Management of Biometric Data in Schools	16
Appendix D –Subject Access Request Management	21
Appendix E – Subject Access Request – Flowchart	25
Appendix F – FOI Policy and Publication Scheme	26
Appendix G – Freedom of Information Request – Flowchart	31
Appendix H - Data Breach Response & Management	32
Appendix I – Data Breach Response – Flowchart	38
Appendix J – Document Retention Schedule	39
Appendix K – Data Sharing Decision Tree	44
Appendix L – New Software and Online Platform Procurement/Adoption Protocol	45
Appendix M – Software and Online Platform Approval -Flowchart	49
Appendix N – DPIA Screening Template: New Software & Digital Platforms	50
Appendix O – Data Protection Impact Assessment (DPIA) Template	52





Appendix P – Consent Form – Parent for Event [2026]	57
Appendix Q – Consent Form – Parent General [2026]	60
Appendix R – Consent Form – Pupil (Age 13+)	62
Appendix S – Pupil & Parent / Carer Privacy Notice	64
Appendix T – Workforce Privacy Notice	70
Appendix U – Supplier & Contractor Privacy Notice	71
Appendix V – Governance Role Privacy Notice (Trustees, Members & Academy Councillors)	78





1. Purpose and Scope

This policy has been equality impact assessed and we believe is in line with the Equality Act 2010.

Shaw Education Trust ("the Trust") is committed to protecting personal data and processing it lawfully, fairly, transparently and securely. This policy establishes the Trust-wide framework for compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Data (Use and Access) Act 2025 and all other applicable legislation and guidance.

This policy applies to all academies, central teams, trustees, governors, volunteers, contractors and third parties processing personal data on behalf of the Trust. It applies to all personal data processed by the Trust including pupil, parent, workforce, safeguarding, SEND, governance, finance, estate management, visitor, supplier, CCTV, biometric, artificial intelligence and information systems data.

2. Legal Framework

This policy has due regard to, but is not limited to:

- UK GDPR
- Data Protection Act 2018
- Data (Use and Access) Act 2025
- Freedom of Information Act 2000
- Protection of Freedoms Act 2012
- Education (Pupil Information) Regulations
- Privacy and Electronic Communications Regulations
- Keeping Children Safe in Education
- ICO Guidance on UK GDPR
- DfE Data Protection in Schools Guidance
- DfE Generative AI in Education Guidance
- DfE Generative AI Product Safety Standards

3. Data Protection Principles

The Trust will apply the UK GDPR principles: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability. The Trust must be able to demonstrate compliance through policies, procedures, records of processing activities, privacy notices, contracts, DPIAs, audits, training records and incident logs.



4. Governance and accountability

The Trust Board retains overall accountability for compliance and assurance. Trustees will receive regular reports regarding, data protection risks, breaches and incidents, information rights performance, DPIAs, supplier assurance, training compliance and audit findings.

The Trust operates a centralised data protection framework. All academies and central teams must comply with Trust-wide policies, procedures and standards. The Trust must be able to demonstrate compliance consistently across all processing activities undertaken throughout the organisation.

The Trust will maintain:

- Records of Processing Activities (ROPA)
- Data maps
- Privacy notices
- Consent records where applicable
- Processor contracts
- DPIAs
- Data breach logs
- Retention schedules.

[See Appendix B – Trust Governance Terms]

5. Roles and responsibilities

Trust Board - The Trust Board retains ultimate accountability for data protection compliance and assurance.

Chief Executive Officer and Executive Leadership Team - Responsible for ensuring sufficient resources, leadership and governance arrangements exist to support compliance.

Director of Data Strategy & Information Systems - Responsible for Trust-wide information governance arrangements, strategic oversight, reporting and implementation of this policy.



Data Protection Officer - The DPO shall:

- Advise on compliance obligations.
- Monitor compliance.
- Support information rights requests.
- Advise on DPIAs.
- Liaise with the ICO.
- Promote privacy awareness.
- Provide training and assurance activities.
- Report risks to senior leaders and Trustees.

Headteacher & Academy Data Protection Leads - Each academy shall nominate an appropriate senior leader responsible for local implementation and evidence of compliance.

All Staff and Volunteers - Must:

- Protect personal data.
- Complete mandatory training.
- Follow Trust procedures.
- Report concerns immediately.
- Use systems responsibly and lawfully

[See Appendix B – Trust Governance Terms]

6. Lawful basis and special category data

All processing activities must have a documented lawful basis before processing begins. Where special category data is processed, a UK GDPR Article 9 condition and relevant Data Protection Act 2018 Schedule 1 condition must also be identified and documented. The Trust may rely upon public task, legal obligation, contract, consent, vital interests and legitimate interests [where appropriate].

Consent must be used only where it is the most appropriate basis, and the individual has a genuine choice. Consent must be freely given, specific, informed, unambiguous, recorded and easy to withdraw. Where processing is required for education, safeguarding, statutory returns, employment, public task or legal obligation reasons, consent will often not be the appropriate basis.

[See Appendix S, T,U & V - Privacy Notices]



7. Transparency and privacy notices

The Trust will maintain clear, accessible privacy notices for pupils, parents/carers, staff, applicants, governors, trustees, volunteers, visitors, contractors, CCTV/image use, AI/EdTech and other relevant processing. Privacy notices will explain why information is collected, identify lawful bases, explain sharing arrangements, state retention periods, explain individual rights and identify the DPO.

8. Children's data and safeguarding

The Trust recognises that children's data requires enhanced protection. Processing must always be lawful, fair, proportionate and in the best interests of the child.

The Trust may share information for safeguarding without consent where necessary to protect a child or comply with safeguarding duties. Information sharing decisions must be documented appropriately by the Designated Safeguarding Lead.

9. Information rights

Individuals, including children, may exercise rights including access, rectification, erasure, restriction, objection, data portability where applicable, withdrawal of consent and rights relating to automated decision-making. Staff must recognise that requests may be verbal or written, including through social media, and must escalate them without delay.

SARs will normally be answered within one calendar month unless an extension is lawful for complex or multiple requests. Identity and authority must be verified before disclosure.

The Trust will maintain a data protection complaints process. It will acknowledge data protection complaints within 30 days throughout the year, including during school holiday periods. The recipient schools Data protection Lead will investigate without undue delay, keep the complainant informed and provide an outcome. Complaints regarding the handling of a SAR will be reviewed by a person not directly involved in the original decision where practicable, at school level. Any appeals regarding a complaint outcome will be escalated to the Trust DPO.

[See Appendix D – Subject Access Request Management]

[See Appendix E – Subject Access Request –Flowchart]

[See Appendix F – FOI Policy and Publication Scheme]

[See Appendix G – Freedom of Information Request –Flowchart]



10. Data sharing, processors and suppliers

Routine controller-to-controller sharing must be supported by a data sharing agreement or documented decision record. Processor arrangements must be covered by written contractual terms that meet UK GDPR requirements, including subject matter, duration, nature, purpose, data types, security, sub-processors, assistance with rights, breach notification, return/deletion and audit/assurance rights.

For EdTech, cloud, AI and other digital tools, the Trust must complete data protection due diligence before procurement or use. The assessment must consider controller/processor status, data categories, lawful basis, special category data, sub-processors, international transfers, security, retention, exit, deletion, pupil safety, DPIA need and privacy notices.

[See Appendix K – Data Sharing Decision Tree]

[See Appendix H – Data Breach Response and Management]

[See Appendix I – Data Breach Response -Flowchart]

See other policies for further information: AI / Data Security

11. Records management, retentions and disposal

The Trust will maintain records of processing activities and data maps covering data subjects, data categories, purposes, lawful bases, special category conditions, recipients, processors, systems, storage locations, transfers, retention periods, security controls and owners.

The Trust will maintain and apply a Data Retention Schedule. Academies and central teams must review personal data at least annually, identify data no longer needed, and dispose of it securely. Destruction must be authorised, documented and carried out so records cannot be reconstructed.

[See Appendix J – Document Retention Schedule]

12. DPIAs and privacy by design

DPIA screening must take place before new or significantly changed processing likely to create high risk. DPIAs are required for high-risk processing such as large-scale special category data, biometric systems, AI tools [including those embedded within existing systems], EdTech, profiling, automated decision-making, safeguarding platforms, CCTV expansion, monitoring, new data sharing or new cloud systems.



DPIAs must describe processing, assess necessity and proportionality, assess risks and record mitigations. Processing must not go live until DPIA actions, contracts, privacy information, security checks and DPO advice have been completed or appropriately risk-accepted by the senior owner.

See other policies for further information: AI / Data Security

[See Appendix M – Software and Online Platform Approval -Flowchart]

[See Appendix O – Data Protection Impact Assessment (DPIA)]

13. Biometrics, photos, videos and CCTV

Biometric recognition systems must not be introduced without DPIA, appropriate lawful basis, Article 9 condition, privacy information, written parental notification/consent requirements, pupil refusal safeguards and reasonable alternatives. A child's refusal overrides parental consent, and biometric data must be securely deleted when no longer needed.

Photos, videos and CCTV involving identifiable individuals are personal data. They must be used lawfully and proportionately, with clear purposes, privacy information/signage, access controls, retention periods and secure storage. CCTV must operate in line with the separate CCTV policy and be reviewed periodically.

[See Appendix C – Information Sheet: Management of Biometric Data in Schools]

14. Artificial Intelligence and Automated Decision-Making

The Trust recognises the opportunities and risks associated with AI technologies. Approved AI tools must comply with applicable legislation and DfE product safety standards and meet the expectations of our trust wide AI Strategy. For further information refer to our Trust AI Strategy document.

Personal data, safeguarding information, SEND information, confidential Trust information, identifiable pupil work or staff data must not be entered into any unapproved AI systems.

AI and EdTech tools must be assessed for data flows, pupil interaction, harmful or biased content, monitoring/supervision, supplier roles, sub-processors, transfers, retention, security and product changes. The DPL, IT/digital lead and DSL at school level must be consulted where risk requires it.



AI systems must not independently make significant decisions relating to admissions, attendance intervention, behaviour sanctions, recruitment, performance management, safeguarding or pupil outcomes without meaningful human review and accountability.

DPIA assessment is required where personal data is processed by AI systems.

15. Information Security and Cloud Computing

The Trust will apply appropriate technical and organisational measures, including access controls, role-based permissions, secure authentication, encryption where appropriate, endpoint protection, secure disposal, logging, backup and recovery, and staff awareness. Staff must follow Trust information security, acceptable use, password, AI, CCTV, breach and retention procedures.

All suspected or actual personal data breaches must be reported immediately through the Trust breach process. The DPO / DPO Service will support containment, risk assessment, ICO notification where required, notification to affected individuals where required, remedial action and lessons learned. Every breach or near miss must be recorded and reviewed for trends.

16. Data breaches and incident management

All suspected or actual personal data breaches must be reported immediately using Trust procedures.

The Trust process will investigate all incidents, assess risk, record lessons learned, implement corrective action and will report breaches to the ICO where required. Where required by law, personal data breaches will be reported to the ICO within 72 hours of becoming aware of the breach.

Affected individuals will be informed where there is a high risk to their rights and freedoms.

17. Training, monitoring and assurance

All staff must complete data protection training on induction and refresher training at least every 2 years, with annual refresher training as Trust best practice and targeted training for higher-risk roles. Training must be completed online using our Trust wide adopted training platform.



The Trust will monitor compliance through audits, ROPA reviews, DPIA review, supplier assurance, SAR and complaint logs, breach analysis, retention checks, access reviews, training records and reporting to senior leaders and Trustees.

18. Related policies

This policy should be read alongside the following: -

- Data Security Policy
- Data Breach Response Plan
- CCTV Policy,
- AI Policy,
- Acceptable Use Policy,
- Password and Access Management Policy,
- Records Retention Schedule,
- FOI Policy and Publication Scheme,
- Privacy Notices,
- Safeguarding and Pupil Protection Policy,
- Complaints Policy and procurement/contract management procedures.

19. Review and approval

This policy will be reviewed annually, or sooner if legislation, statutory guidance, ICO guidance, DfE guidance, Trust structure, systems or processing risks materially change.

The Trust Board is responsible for approval of this policy.



Appendix A – Glossary of Terms

Academy Data Protection Lead (DPL)	The nominated individual within an academy responsible for supporting local compliance with Trust data protection requirements, liaising with the Trust DPO and maintaining local evidence of compliance.
Artificial Intelligence (AI)	Technology capable of performing tasks that normally require human intelligence, such as generating content, analysing data, recognising patterns or supporting decision-making. Within the Trust, all AI use must comply with applicable legislation, Trust policies and governance requirements.
Automated Decision-Making	A decision made solely by automated means, without meaningful human involvement, which produces legal or similarly significant effects for an individual.
Biometric Data	Personal data resulting from specific technical processing relating to an individual's physical, physiological or behavioural characteristics that enables unique identification, such as fingerprint recognition or facial recognition.
Cloud Computing	The provision of computing services, applications and data storage through internet-based platforms rather than local infrastructure. Examples include Microsoft 365, Azure and cloud-hosted management systems.
Consent	A freely given, specific, informed and unambiguous indication of an individual's wishes by which they agree to the processing of their personal data. Consent must be capable of being withdrawn.
Controller	The organisation or body that determines the purposes and means of processing personal data. Shaw Education Trust is the Data Controller for personal data processed by its academies and central services.
Data Protection Impact Assessment (DPIA)	A process used to identify, assess and mitigate privacy risks associated with new projects, technologies, systems or processing activities involving personal data.
Data Processor	An organisation or individual that processes personal data on behalf of a Data Controller. Examples may include software suppliers, hosted services and outsourced providers.
Data Sharing Agreement (DSA)	A documented agreement setting out the purpose, legal basis, responsibilities and safeguards for the routine sharing of personal data between organisations acting as separate controllers.



Data Subject	A living individual who can be identified, directly or indirectly, from personal data. Examples include pupils, parents, staff, volunteers, governors, trustees and contractors.
Data Breach (Personal Data Breach)	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
Data Mapping	The process of identifying, documenting and understanding what personal data is held, where it is stored, how it flows through systems, who accesses it and how long it is retained.
Data Minimisation	The principle that personal data collected and processed must be adequate, relevant and limited to what is necessary for the stated purpose.
Data Protection Officer (DPO)	The individual or appointed service responsible for advising on data protection obligations, monitoring compliance, supporting data subjects, advising on DPIAs and acting as the primary contact with the Information Commissioner's Office (ICO).
DfE	The Department for Education, responsible for education policy, guidance and regulation in England.
Freedom of Information (FOI)	The legal right for individuals to request recorded information held by public authorities, including academy trusts, subject to statutory exemptions.
Generative AI	A form of artificial intelligence capable of creating new content such as text, images, audio, code or analytical outputs in response to prompts provided by users.
Information Commissioner's Office (ICO)	The UK's independent supervisory authority responsible for regulating and enforcing data protection legislation and freedom of information legislation
Information Rights	The legal rights individuals have regarding how organisations process their personal data, including rights of access, rectification, erasure, restriction, objection and portability
International Transfer	The transfer of personal data outside the United Kingdom, which requires appropriate safeguards and legal mechanisms to protect personal data.
Lawful Basis	The legal justification under UK GDPR for processing personal data, such as public task, legal obligation, contract, consent, vital interests or legitimate interests.
Personal Data	Any information relating to an identified or identifiable living individual. This includes names, addresses, identification numbers, online identifiers and other information capable of identifying a person.



Privacy Notice	A document explaining how personal data is collected, used, shared, stored and protected, and outlining the rights available to individuals.
Privacy by Design	An approach requiring privacy and data protection considerations to be embedded into projects, systems and processing activities from the outset rather than applied retrospectively.
Processing	Any operation performed on personal data, including collection, recording, organisation, storage, retrieval, consultation, sharing, amendment and deletion.
Profiling	Any form of automated processing used to evaluate, analyse or predict aspects relating to an individual's performance, behaviour, preferences, interests or circumstances.
Record of Processing Activities (ROPA)	The Trust's documented record of personal data processing activities, including purposes, lawful bases, categories of data, recipients, retention periods and security measures.
Special Category Data	Particularly sensitive personal data requiring additional protections, including information relating to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, genetics, biometrics, sex life or sexual orientation.
Subject Access Request (SAR)	A request made by an individual seeking access to personal data held about them by the Trust.
UK GDPR	The United Kingdom General Data Protection Regulation, which governs the processing of personal data within the UK and establishes rights for individuals and responsibilities for organisations.
UK Data Protection Legislation	Collectively refers to UK GDPR, the Data Protection Act 2018, the Data (Use and Access) Act 2025 and associated legislation and guidance applicable to the Trust.



Appendix B – Trust Governance Terms

Academy Council	The local governance body established by the Trust to support and challenge academy leadership, provide local oversight and represent stakeholders in accordance with the Scheme of Delegation. Academy Councils operate under powers delegated by the Trust Board.
Academy Data Protection Lead (DPL)	The nominated individual within an academy responsible for supporting local compliance with Trust data protection requirements, coordinating local responses to incidents and requests, maintaining compliance evidence and acting as the primary liaison with the Trust's DPO service.
Central Team	Employees working in Trust-wide service functions such as data, IT, finance, HR, estates, governance, marketing and school improvement who provide services across multiple academies.
Chief Executive Officer (CEO)	The Accounting Officer and senior executive responsible for the overall leadership, management and performance of Shaw Education Trust, including ensuring appropriate arrangements are in place for information governance and data protection compliance.
Data Governance	The framework of policies, standards, processes, controls and assurance activities used to ensure personal and organisational data is managed lawfully, securely, consistently and effectively across the Trust.
Director of Data Strategy & Information Systems	The Trust's strategic lead for data, information governance, business intelligence, information systems, reporting, data architecture and digital information management. The role supports Trust-wide oversight of data governance, compliance and data strategy.
Data Protection Officer (DPO)	The independent individual or contracted service appointed by the Trust to advise on data protection obligations, monitor compliance, support information rights, advise on DPIAs and act as the primary contact with the Information Commissioner's Office (ICO). The DPO reports independently and must not be subject to conflicts of interest.
DPO Service	The external or internal arrangement through which Data Protection Officer responsibilities are delivered to the Trust, including compliance advice, assurance, information rights support, incident management advice and regulatory liaison.
Executive Leadership Team (ELT)	The group of senior leaders responsible for the strategic and operational leadership of the Trust. ELT provides oversight of



	risk, compliance, digital transformation and organisational performance.
Information Asset Owner (IAO)	A senior individual responsible for overseeing a specific information asset, system or dataset, ensuring appropriate security, retention, access controls, compliance and accountability arrangements are maintained.
Local Compliance Evidence	The records, logs, training records, audits, assessments and other documentation maintained by academies to demonstrate compliance with Trust data protection requirements and statutory obligations.
Record of Processing Activities (ROPA)	The Trust-wide record maintained to document processing activities, lawful bases, data categories, recipients, retention periods, security controls and ownership responsibilities.
Senior Leadership Team (SLT)	The leadership team operating within an individual academy and responsible for implementing Trust policies, ensuring local compliance and managing day-to-day operational risks relating to personal data.
Scheme of Delegation	The Trust governance document which sets out how decision-making powers, responsibilities and accountabilities are delegated by the Trust Board to committees, Academy Councils, executive leaders and academy leaders.
Trust Board	The legal governing body and Data Controller for Shaw Education Trust. The Trust Board retains ultimate accountability for governance, strategic direction, risk management, statutory compliance and data protection assurance across all academies and central services.
Trust Information Governance Framework	The collection of policies, standards, procedures, registers, records and assurance mechanisms that collectively support information governance, data protection, cyber security, records management and compliance across the Trust.
Trustee	A member of the Trust Board with legal responsibility for the governance and strategic oversight of Shaw Education Trust. Trustees have collective accountability for ensuring appropriate systems of compliance, assurance and risk management.



Appendix C

Information Sheet: Management of Biometric Data in Schools

Document type:	Information governance guidance
Owner:	Director of Data Strategy and Information Systems
Applicable to:	All academies and central teams
Review Frequency:	Annual

1. Purpose

This information sheet provides guidance on the lawful collection, use, storage and deletion of biometric data within Shaw Education Trust. The Trust recognises that biometric information is particularly sensitive and requires enhanced safeguards due to the potential impact on individual privacy and personal rights.

This guidance supports compliance with:

- UK GDPR
- Data Protection Act 2018
- Protection of Freedoms Act 2012
- Department for Education guidance
- Shaw Education Trust Data Protection Policy.

2. What is Biometric Data?

Biometric data is personal information obtained through technical processing of an individual's physical, physiological or behavioural characteristics that enables unique identification. Examples include Fingerprint recognition, Finger geometry recognition, Facial recognition, Iris scanning, Voice recognition

In schools, biometrics are most commonly used for Cashless catering systems, Library systems, Secure printing systems, Access control systems, and Registration systems.

3. Special Category Data

Biometric data used for identification purposes is classified as Special Category Personal Data under UK GDPR.

As a result: additional legal protections apply, stronger security controls are required, a Data Protection Impact Assessment (DPIA) is usually required, and explicit consent arrangements may be required depending on the processing activity.

4. Trust Requirements Before Introducing a Biometric System

No academy may introduce a biometric recognition system without first:





Step 1 – Business Need Assessment

The academy must demonstrate:

- A genuine operational need.
- That the intended use is proportionate.
- That less intrusive alternatives have been considered.

Examples of acceptable reasons may include:

- Reducing cash handling.
- Improving service efficiency.
- Reducing administrative burden.

Step 2 – Data Protection Impact Assessment

A DPIA must be completed before implementation.

The DPIA should assess privacy risks, security risks, safeguarding implications, alternative options, retention periods supplier arrangements and individual rights.

The DPIA must be reviewed by the DPO or DPO Service before implementation.

Step 3 – Supplier Due Diligence

- Prior to procurement the academy must ensure:
- Appropriate contracts are in place.
- Security controls are documented.
- Data storage locations are known.
- International transfers are assessed.
- Retention arrangements are understood.
- Deletion arrangements are confirmed.

The supplier must demonstrate UK GDPR compliance.

5. Parental Notification Requirements

Before processing biometric data relating to a pupil under 18 years of age the academy must notify all individuals with parental responsibility that:

- The academy intends to collect biometric information.
- The purpose of collection.
- How the information will be used.
- How long the information will be retained.



- The rights available to parents and pupils.

Notification should be issued before any biometric data is collected.

6. Obtaining Consent

The school must obtain appropriate written consent before processing pupil biometric information.

The consent process must be clear and understandable, explain the intended use, not be bundled with unrelated permissions and be easy to withdraw.

Records of consent must be maintained and auditable.

7. Pupil Objection Rights

Regardless of parental consent a pupil's objection overrides consent. A biometric system must not be used where a pupil refuses to participate, expresses an objection or withdraws participation.

This applies even if parental consent has previously been obtained.

8. Alternative Arrangements

Schools must provide a reasonable alternative for any pupil who does not consent, withdraws consent, objects to participation or is unable to use the biometric system.

Examples include PIN numbers, Swipe cards, Barcode cards or Manual identification methods.

Pupils must not be disadvantaged because they do not participate in biometric processing.

9. Security Requirements

Academies must ensure biometric data is protected using appropriate technical and organisational measures. This should include:

- Encryption.
- Role-based access control.
- Strong authentication.
- Audit logging.
- Secure backups.
- Restricted administrator access.

Access should be limited to authorised staff with a legitimate need.



10. Data Retention

Biometric information must only be retained while required for the identified purpose and the pupil or individual remains a user of the service.

Biometric templates must be securely deleted when:

- A pupil leaves the academy.
- Consent is withdrawn.
- The service ceases.
- The information is no longer required.

The academy must be able to demonstrate secure deletion.

11. Staff Biometric Data

Where biometric systems are used for staff explicit consent must be obtained where required participation must be voluntary where consent is relied upon, alternative processes must be available and privacy information must be provided.

Biometric systems must not be implemented simply for staff convenience where less intrusive alternatives are available.

12. Subject Access Requests and Rights

Individuals may exercise their rights under data protection legislation including:

- Right of access.
- Right to rectification.
- Right to object.
- Right to erasure where applicable.
- Right to restrict processing.

All requests must be referred immediately to the Academy Data Protection Lead and DPO Service.

13. Data Breaches

Any actual or suspected breach involving biometric information must be reported immediately through the Trust's Data Breach Procedure.

Examples include lost equipment, unauthorised access, incorrect disclosure, cyber-attack or supplier security incident.

Due to the sensitive nature of biometric information, breaches involving biometric data require urgent escalation.



14. Academy Compliance Checklist

Before using biometric technology, schools must confirm:



Business need established	
Alternative solutions considered	
DPIA completed	
DPO consulted	
Supplier due diligence completed	
Appropriate contract in place	
Privacy notice updated	
Parent notification completed	
Consent process implemented	
Alternative arrangements available	
Retention period established	
Deletion process documented	
Security controls assessed	
Staff training completed	
Incident reporting process understood	

Information shared in this information sheet was correct at time of publication, any changes to legislation will be considered and this document updated accordingly as and when required, but reviewed, as a minimum, on an annual basis.



Appendix D – Subject Access Request Management

Document type:	Process guidance
Owner:	Director of Data Strategy and Information Systems
Applicable to:	All academies and central teams
Review Frequency:	Annual

1. Purpose

This guidance document outlines the Trust process regarding the handling of subject access requests and applies to all academies and central teams.

Due to the wide range of information requests academies and central teams receive, this document may not address every specific question, however it does provide an overview of each agreed step in our Trust process and some guidance on where additional support can and should be sought.

2. Who is the Data Protection Lead for schools

The Data Protection Lead [DPL] is the nominated individual within an academy responsible for supporting local compliance with Trust data protection requirements, coordinating local responses to incidents and requests, maintaining compliance evidence and acting as the primary liaison with the Trust's DPO / DPO service.

All information requests received, via whatever means, will be shared with the Academy DPL, who is responsible for the management of the process.

3. What is a Subject Access Request?

A subject access request [SAR] is a formal request made under data protection law [UK GDPR] that allows an individual, such as a parent, pupil or staff member, to ask for a copy of the personal data the Trust holds about them or their child.

Our Trust is committed to being inclusive and accessible to our whole school community. To ensure no one faces barriers when exercising their data rights, we do not use a standardised template. We accept Subject Access Requests in any format. This includes emails, written letters, verbal requests, and messages sent via our official social media channels.



4. Information request assessments

Due to the variety of requests received by schools, **RECOGNISING** a request has been made is the first step. All Academies should provide training to staff on what constitutes an information request and who the Academy Data Protection Lead is.

All requests for information will be shared with the Academy DPL for review. The DPL is responsible for assessing all requests and if additional information is required will seek clarity from the requester.

Below are some of the most common request types:

- **Access:** Requesting a copy of personal data.
- **Erasure:** Asking for data to be deleted (only applies in certain cases).
- **Restriction:** Limiting the use of their data.
- **Rectification:** Correcting incorrect or incomplete data.
- **Portability:** Requesting data be transferred in a structured format.
- **Objection:** Asking to stop processing their data.
- **Pupil Record:** Parents requesting only the educational record.
- **Data Sharing:** External organisations (e.g., police) requesting data - requires careful validation.

The Academy DPL is responsible for **RECORDING** the information request on the Trust adopted platform which is GDPRiS <https://identity.gdpr.school/Login>. If the DPL is experiencing any problems accessing the site, please follow our Trust Digital Policy and raise a ticket for support with our IT Helpdesk.

GDPRiS information requests should be raised by the DPL and should include as much information as possible about the request made.

The DPL will **Respond** to all requests with an acknowledgment and an estimated timeframe for full response. Use this response to seek any further clarifications regarding the request and request proof of ID [if necessary]. All requests will be responded to within 30 days of receipt of the request and following any further clarification of the request and ID checking has taken place. Where the request is deemed to be complex and have multiple elements the response period may be extended by up to two further months, please see latest ICO guidance for further information.



All requests will be **Reviewed** using the **C.A.R.E** system.

C	Conflicts	Situations that may restrict access to all or parts of the request (e.g. court orders, safeguarding concerns).
A	Age	Assess if the requester is old enough to make the request and more importantly if they are competent to do so.
R	Responsibility	Verify parental responsibility or legal authority. Do you need to confirm if they are working on behalf of the data subject?
E	Exemptions	Check ICO guidelines for legal exemptions (e.g. safeguarding, confidentiality).

Once reviewed, the DPL may have grounds to **REJECT** part or all the request. Requests can be refused for valid reasons, such as: -

- **Excessive or malicious requests** – Seek guidance from DPO service to verify
- **A competent child refusing parental access** – Seek guidance from DPO service

If a request is being rejected it is the DPL's responsibility to inform the requester of the reason, provide ICO complaint details and maintain records within GDPRiS platform to ensure accurate recording.

All data will be checked prior to being shared with the requester. Any data which is not related to the Data subject must be **REDACTED**. The following approach to redaction should be applied, wherever necessary seek advice from the DPO / DPO service prior to sharing with requester.

AI tools are not permitted for redaction purposes, due to the sensitivity of the data, this data should not be uploaded to any AI tools. Due to the meticulous nature of this task, this is best completed by the DPL or delegated under supervision to another member of Academy staff.

REDACTION

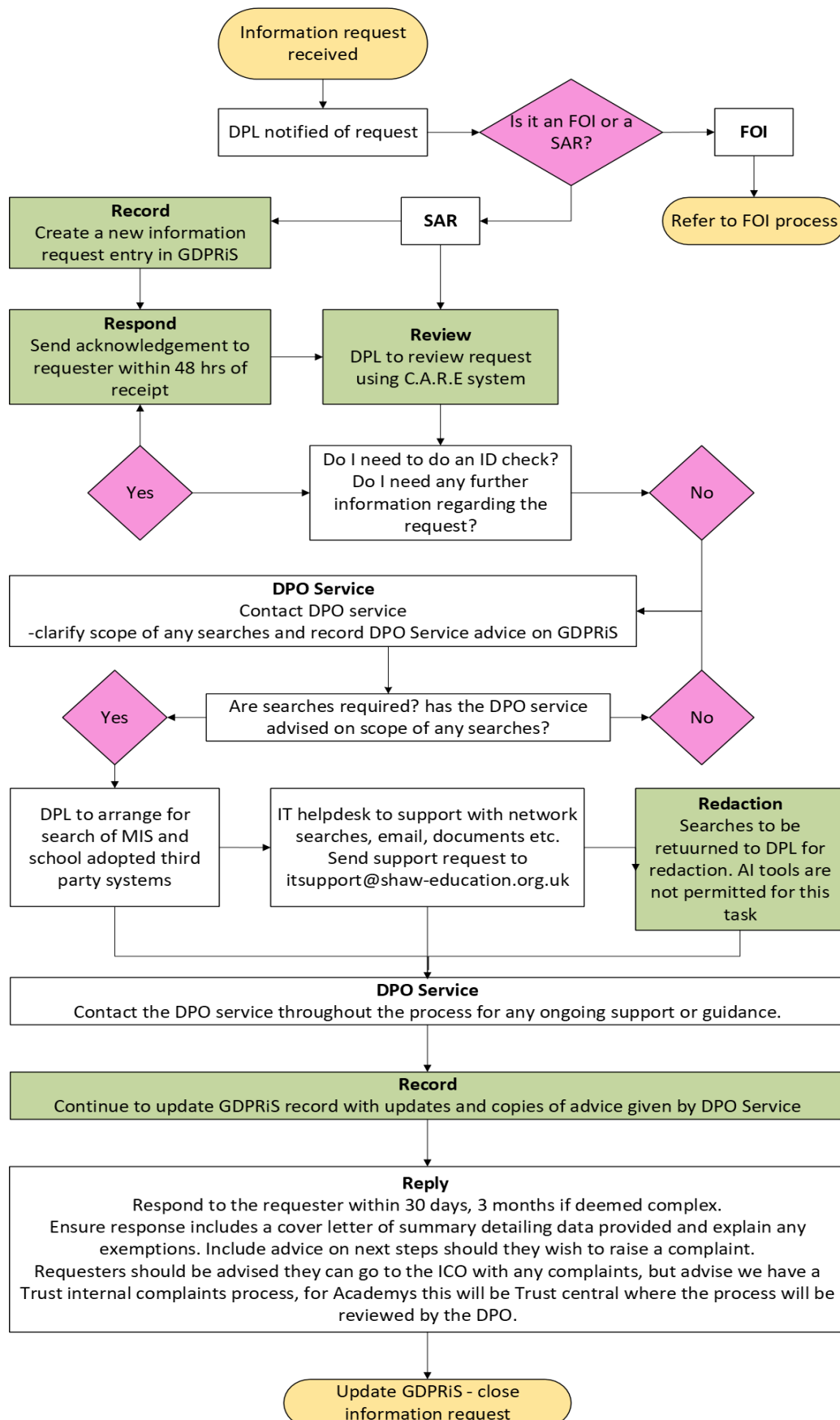
- a. Data does not have to be obvious:
 - **Direct data** - Clearly belongs to someone else – must be redacted
 - **Indirect data** - Information that could reveal someone's identity through context - assess if redaction is needed. DPL liaise with DPO service.
- b. If it does contain other individuals' data, consider
 - Are they an education, social or health worker?
 - Is it reasonable to get consent
 - Would it be reasonable to disclose
 - When in doubt, **REDACT**.



Once a request has been considered and the DPL is ready to share the information with the requester, the DPL will **REPLY** with the appropriate information. Send the requested data using the same method it was received unless otherwise specified. Including a cover letter summarising the data provided and explain what exemptions you have used providing by doing so you are not causing further safeguarding issues.



Appendix E – Subject Access Request – Flowchart





Appendix F – FOI Policy and Publication Scheme

Document type:	Process guidance – Freedom of information act 2000
Owner:	Director of Data Strategy and Information Systems
Applicable to:	All academies and central teams
Review Frequency:	Every two years

FOI Policy

1. Purpose

Shaw Education Trust [The Trust] is committed to openness, transparency and accountability. This policy explains how individuals may request information held by the Trust under the Freedom of Information Act 2000 (FOIA) and how the Trust will respond to such requests.

The policy also incorporates the Trust's Publication Scheme, detailing information routinely made available without the need for a formal FOI request.

2. Scope

This policy applies to:

- The Trust Board
- Central Trust services
- All academies and schools within the Trust
- Employees
- Trustees and Governors
- Contractors acting on behalf of the Trust where information is held for Trust purposes

b. What is Freedom of Information?

The Freedom of Information Act 2000 gives any person the right to request recorded information held by public authorities, including academies and multi-academy trusts.

Information may be requested regardless of the applicants age, nationality, place of residence or reason for requesting the information. The applicant does not need to explain why the information is required.

c. Distinguishing FOI request from Subject Access Requests

Freedom of Information requests relate to information held by the Trust.



Subject Access Requests (SARs) relate specifically to personal data concerning the requester. Where a request includes personal information about an identifiable individual, the Trust will determine whether the request should be handled under UK GDPR and Data Protection legislation as a SAR or the request should be handled under FOIA. Where there is uncertainty, advice will be sought from the Trust DPO or DPO Service.

d. Receiving requests

FOI requests may be received by email, letter, online form [where available] or any written correspondence.

Any requests received should be forwarded immediately to the schools Data Protection Leader [DPL] for review. All requests must be logged within GDPRiS as a new information request.

e. Validity of requests

To be valid under FOIA, a request must be in writing, include the applicants real name, include correspondence contact details and clearly describe the information requested. Where clarification is required, the DPL may contact the applicant. If further clarification is sought the statutory response time is paused until a response is received.

f. FOI request process

Upon receipt of a valid request the Academy DPL, or nominated central DPL, will follow stages as described within the FOI – Flowchart [attached]. The DPO service will be consulted prior to responses being sent and for any advice or guidance.

3. Information Not Held

Where searches identify that the Trust does not hold the requested information the applicant will be informed promptly and the request record will be updated and closed within GDPRiS. Where appropriate, applicants may be directed to another organisation likely to hold the information.

4. Exemptions

FOIA recognises circumstances where information may legitimately be withheld. Examples include:

Absolute Exemptions

- Information accessible by other means
- Personal information
- Court records
- Information provided in confidence

Qualified Exemptions



- Commercial interests
- Legal professional privilege
- Health and safety
- Future publication
- Prejudice to the effective conduct of public affairs

Where a qualified exemption applies, the Trust will undertake a Public Interest Test. If an Academy DPL deems a request to be exempt, guidance will be sought from the DPO Service or Trust appointed DPO.

5. Vexatious or Repeated Requests

The Trust may refuse requests where they are vexatious; they impose a disproportionate burden; or they repeat similar requests previously answered.

Such decisions shall be documented and approved by the Trust appointed DPO.

6. Charges

Most information will be provided free of charge. Where permitted by legislation, charges may be applied for printing, postage, photocopying or large-scale reproduction. Applicants will be informed before any charge is incurred.

7. Internal Review

Applicants dissatisfied with a response may request an internal review within 40 working days. The review will:

- Be conducted by an individual not involved in the original decision wherever possible.
- Consider whether FOIA requirements were properly applied.
- Be completed within a reasonable timescale.

8. Information Commissioner's Office

Applicants who remain dissatisfied may complain to:

Information Commissioner's Office (ICO)

Website: <https://ico.org.uk>

The Trust encourages applicants to complete the internal review process before approaching the ICO.



Publication Scheme

1. Introduction

The Trust adopts the Information Commissioner's Model Publication Scheme and is committed to proactively making information available to the public wherever possible. Information will be published through:

- Trust website
- School websites
- Annual reports
- Statutory disclosures
- Financial returns

2. Classes of information

Class	Includes	Availability: HC = Hardcopy W = Website
Class 1: Who we are and what we do	• Governance structure • Trust Board membership • Committee structures • Senior leadership arrangements • Academy details – school day times and term dates • Organisational charts	W W W W W & HC W
Class 2: What we spend and how we spend it	• Audited accounts • Annual reports • Pay policy • Funding agreements • Procurement information • Financial regulations	W & HC W & HC HC W & HC W & HC W & HC
Class 3: What our priorities are and how we are doing	• Trust Development Plan • School improvement priorities • Performance information • Ofsted reports • Annual objectives	HC HC W & HC W W
Class 4: How We Make Decisions	• Trustee meeting agendas • Approved minutes • Governance policies	W & HC W & HC W & HC



	Where publication is lawful and appropriate.	
Class 5: Policies and procedures	• Data Protection Policy • Freedom of Information Policy • Complaints Procedure • Admissions Policies • Safeguarding Policies • Health and Safety Policies • Staff Codes of Conduct • Equality Information	W & HC W & HC W & HC W & HC W & HC W & HC W & HC W & HC
Class 6: Lists and registers	• Register of trustees • Register of interests • Governance attendance records Subject to legal disclosure requirements.	W & HC HC HC
Class 7: Services we offer	• Educational services • Admissions information • SEND provision information • Community engagement services • Academy contact details	W W & HC W W W

3. Availability of Information

Information will normally be available, via the Trust website; via school websites; upon request by email; or in paper format where appropriate.

4. Monitoring and Review

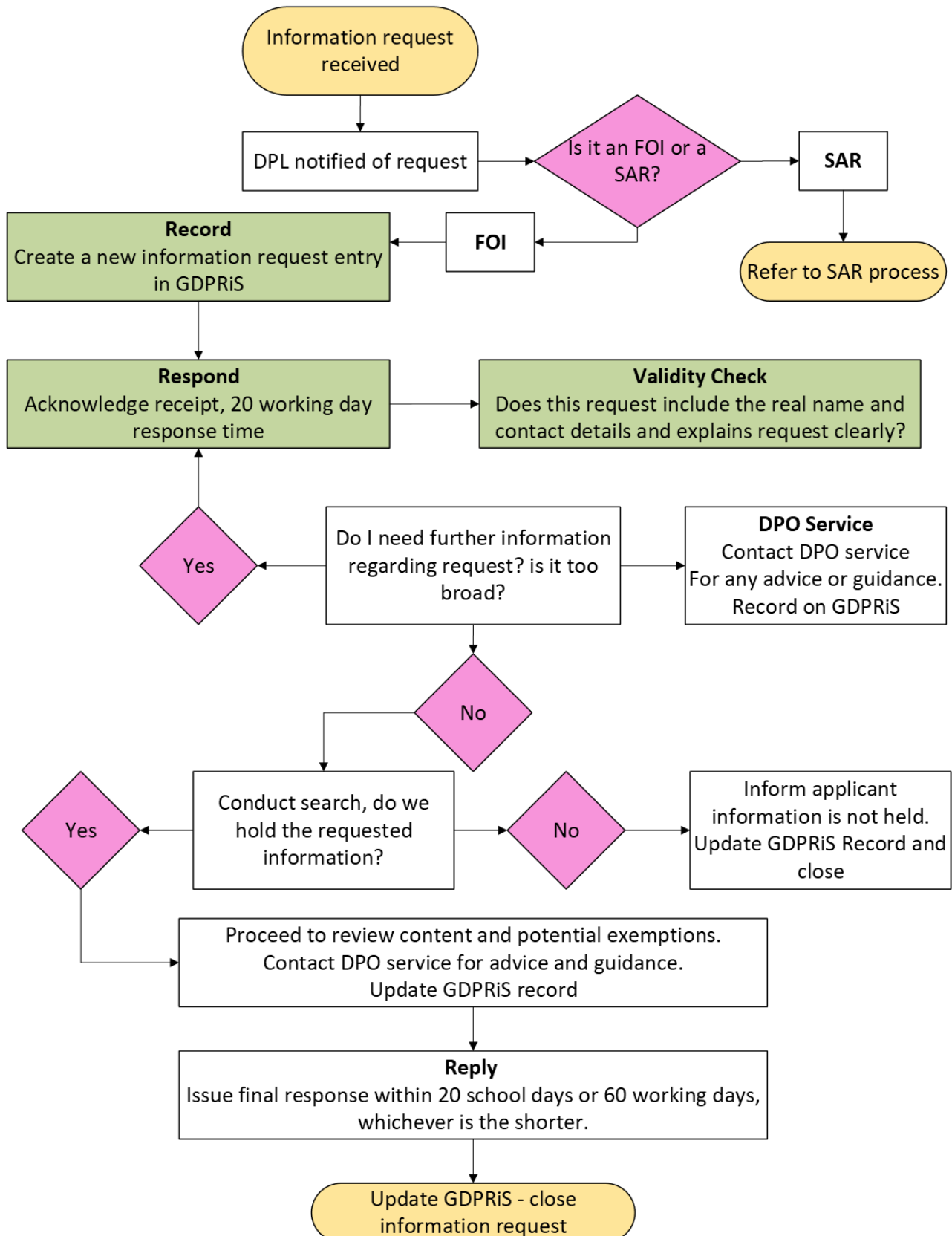
The Trust will periodically review

- Response times;
- Compliance levels;
- Publication Scheme content;
- Requests received;
- Exemptions applied.

Learning from FOI requests will be used to identify information that should be proactively published in the future.



Appendix G – Freedom of Information Request – Flowchart





Appendix H – Data Breach Response & Management

Document type:	Procedural guidance
Owner:	Director of Data Strategy and Information Systems
Applicable to:	All academies and central teams
Review Frequency:	Annual

1. Purpose

The purpose of this procedure is to ensure the Trust responds promptly, consistently and effectively to any suspected or confirmed personal data breach.

The procedure establishes clear responsibilities for reporting, containing, assessing, recording, investigating and learning from data breaches to minimise harm to individuals and ensure compliance with data protection legislation.

All personal data breaches, including near misses and incidents which are found not to be reportable, must be recorded and reviewed within our trust wide adopted platform; GDPRiS.

2. Scope

This procedure applies to:

- All Trust employees
- Trustees and Governors
- Volunteers
- Contractors
- Agency staff
- Third parties processing personal data on behalf of the Trust

The procedure applies to all personal data held by the Trust in:

- Electronic systems
- Cloud platforms
- Paper records
- Portable devices
- Email systems
- CCTV systems
- Biometric systems
- AI and educational technology platforms



3. Definition of a Personal Data Breach

A personal data breach is defined under UK GDPR as "A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data."

Examples include:

Confidentiality Breaches

- Email sent to the wrong recipient
- Unauthorised access to records
- Lost or stolen files
- Data disclosed to an unauthorised third party

Integrity Breaches

- Unauthorised amendment of records
- Corruption of data
- Incorrect information being shared

Availability Breaches

- Accidental deletion of records
- Ransomware attacks
- System failures preventing access to information

The DPO service should be consulted for further information.

4. Responsibilities

All staff	All staff must: • Report suspected breaches immediately. • Cooperate with investigations. • Take immediate actions to limit further exposure where safe to do so. • Preserve evidence. Failure to report a breach promptly may result in disciplinary action.
Academy Data Protection Lead [DPL]	The Academy DPL is responsible for: • Coordinating the local response. • Recording actions taken. • Liaising with the Trust-appointed DPO and DPO service. • Ensuring GDPR records are maintained. • Supporting investigations.
Trust Appointed DPO	The Trust-appointed DPO is responsible for: • Assessing breach severity. • Determining whether ICO notification is required. • Determining whether affected individuals must be informed. • Providing specialist advice / seeking advice through DPO service • Monitoring compliance with statutory requirements. The decision whether a breach requires reporting to the ICO remains the responsibility of the DPO or nominated deputy





5. Reporting a Suspected Breach

Any individual who becomes aware of a suspected breach must immediately:

1. Notify their Academy DPL.
2. Preserve all relevant evidence.
3. Avoid deleting or altering information.
4. Take immediate containment actions where appropriate.

Examples include:

- Recalling emails.
- Retrieving documents.
- Disconnecting compromised devices.
- Changing passwords.
- Restricting system access.

The priority is to prevent further compromise and preserve evidence for investigation. The Academy DPL is responsible for recording the suspected breach and maintaining all investigation information on the trust wide platform GDPRiS.

6. Out of Hours and School Holiday Incidents

Where a breach occurs outside normal school operating hours the nominated on-call contact must be notified immediately, the Trust-appointed DPO and DPO service must be informed at the earliest opportunity, and containment actions must not be delayed.

The Trust must maintain suitable escalation arrangements during weekends, closures and school holidays.

7. Containment and Initial Response

The Academy DPL and relevant support teams will take reasonable steps to contain the breach. This may include:

Technical Measures

- Disabling accounts
- Blocking access
- Isolating devices
- Disconnecting systems
- Recovering deleted information

Physical Measures

- Recovering documents
- Securing filing systems
- Restricting access to locations



Administrative Measures

- Contacting recipients
- Requesting deletion of information
- Obtaining confirmation of destruction

All actions taken must be documented within GDPRiS.

8. Risk Assessment

The DPL and DPO service must assess the seriousness of the breach. Consideration should include:

Volume

- How much data is involved?

Sensitivity

- Does the breach involve special category data?
- Does the breach involve safeguarding information?
- Does the breach involve financial or health information?

Impact

- Could individuals suffer harm?
- Could individuals suffer discrimination?
- Could identities be stolen?
- Could safeguarding risks arise?

Scope

- Single incident or ongoing issue?
- Is the breach fully contained?

The outcome of the assessment must be recorded.

9. ICO Notification

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the Trust must notify the Information Commissioner's Office (ICO). This notification must take place without undue delay and, where feasible, within 72 hours of becoming aware of the breach.

If notification is delayed beyond 72 hours, reasons for the delay must be documented. The ICO notification will normally be coordinated through the DPO service and authorised by the Trust-appointed DPO. There is no requirement for Academy DPLs to take direct action to notify the ICO.

10. Notification to Affected Individuals

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, affected persons must be informed without undue delay.



Notifications should include:

- A description of what happened.
- The data involved.
- Potential consequences.
- Actions already taken.
- Recommended actions individuals should take.
- Contact information for obtaining support.

Examples of actions individuals may need to take include:

- Changing passwords.
- Monitoring accounts.
- Contacting their bank.
- Remaining alert to phishing attempts.

11. Recording Requirements

Every suspected or confirmed breach must be recorded within GDPRiS.

Records must include:

- Date and time discovered.
- Date and time reported.
- Nature of breach.
- Categories of personal data involved.
- Individuals affected.
- Risk assessment outcome.
- ICO notification decision.
- Advice received from DPO service.
- Copies of correspondence.
- Corrective actions implemented.

This applies whether or not the breach is reported externally.

12. Investigation and Root Cause Analysis

Following containment, a formal review must determine the primary cause.

Categories include human error, examples: misdirected email, printing errors, incorrect sharing permissions and failure to follow procedures. System failure, examples: software defects, security vulnerabilities, hardware failures and integration failures.

Many incidents involve both human and technical causes, combined factors.

The investigation findings must be documented within GDPRiS.

13. Corrective and Preventative Actions

The Trust will implement proportionate measures to reduce the likelihood of recurrence.

Measures may include the following:



Human Error Mitigations

- Staff retraining
- Awareness campaigns
- Procedure updates
- Review of access permissions

Technical Mitigations

- Security improvements
- System configuration changes
- Additional monitoring
- Enhanced authentication controls

Governance Improvements

- Policy revisions
- Supplier assurance reviews
- Process redesign

14. DPIA and Risk Review

Where a breach identifies weaknesses in processing activities, the Trust may conduct a review of an existing DPIA, complete a new DPIA, or a wider assessment of organisational controls. The purpose is to identify underlying risks and ensure appropriate mitigations are implemented.

15. Closure

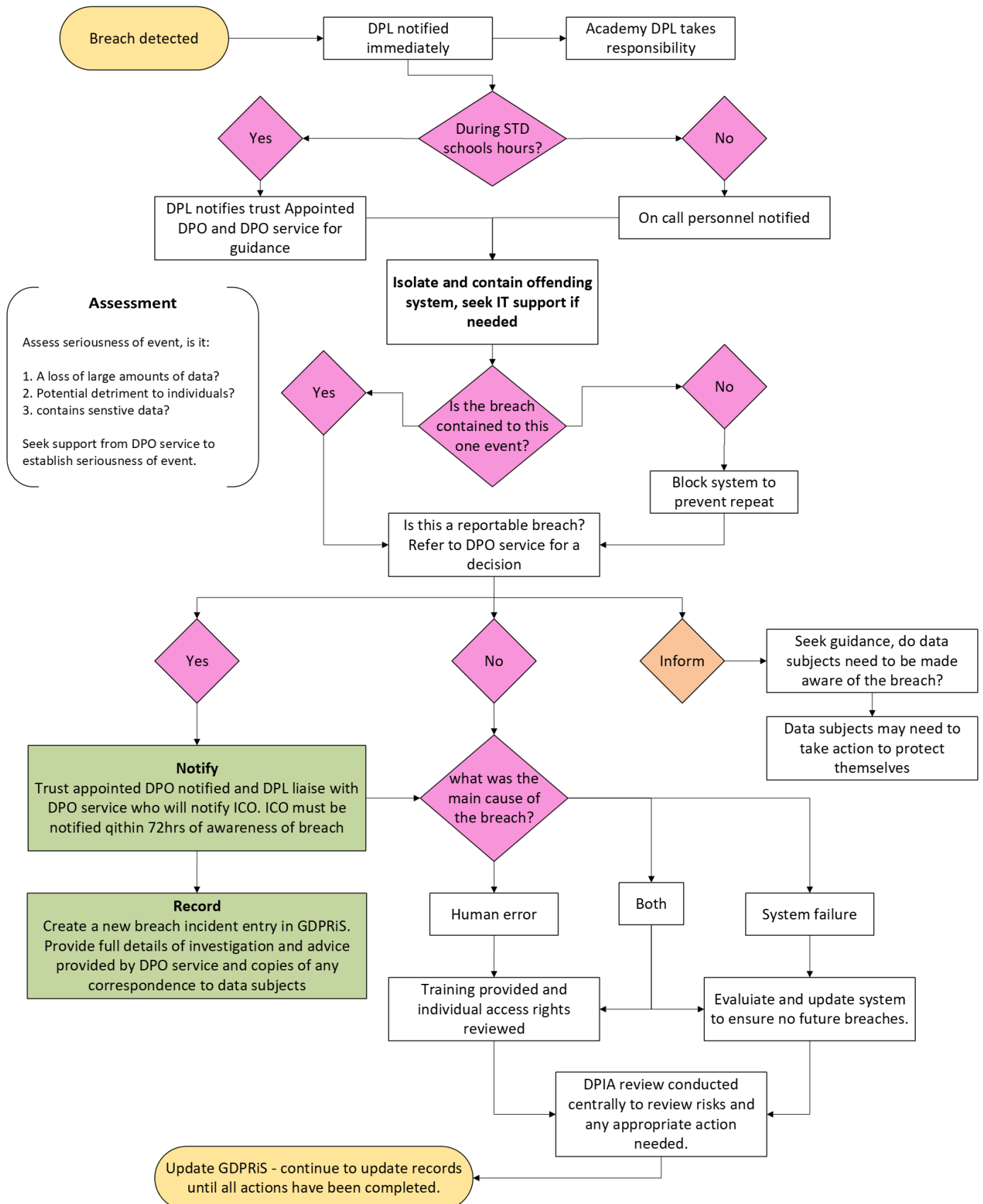
A breach may only be closed when:

- Containment actions are complete;
- Required notifications have been made;
- Investigations have concluded;
- Corrective actions have been agreed;
- GDPRiS records have been updated.

The breach record shall remain open until all actions are completed and evidence has been retained.



Appendix I – Data Breach Response - Flowchart





Appendix J – Information Asset and Retention Schedule

Document type:	Procedural guidance
Owner:	Director of Data Strategy and Information Systems
Applicable to:	All academies and central teams
Review Frequency:	Annual

Retention Principles

All retention periods represent minimum retention requirements. Records may only be retained beyond the specified period where:

- A legal hold applies.
- Litigation is anticipated or ongoing.
- A public inquiry is underway.
- A Subject Access Request, FOI request or complaint is ongoing.
- Regulatory investigation requirements apply.

At the expiry of a retention period, records should either:

- be securely destroyed;
- be anonymised;
- be transferred to an archive; or
- be permanently preserved where historical value exists.

1. Governance and Trust Records

Record Category	Retention Period	Disposal Action
Trust Board minutes (approved)	Permanent	Archive
Trust Board papers	Permanent	Archive
Committee minutes	Permanent	Archive
Committee papers	Current year + 6 years	Secure disposal
Scheme of Delegation versions	Permanent	Archive
Articles of Association	Permanent	Archive
Governance reviews	6 years	Secure disposal
Complaints dealt with by trustees	Resolution + 6 years	Secure disposal
Strategic plans	Superseded + 6 years	Archive review



2. Data Protection and Information Governance

Record Category	Retention Period	Disposal Action
Subject Access Requests (SARs)	Closure + 3 years	Secure disposal
Information Rights requests	Closure + 3 years	Secure disposal
Data breach records	Closure + 6 years	Secure disposal
ICO correspondence	Closure + 6 years	Secure disposal
DPIAs	Life of processing activity + 6 years	Secure disposal
Privacy notices	Superseded + 6 years	Archive one approved copy
Data sharing agreements	Expiry + 6 years	Secure disposal
ROPA records	Life of activity + 6 years	Secure disposal
Information Asset Register entries	Life of asset + 6 years	Secure disposal
Data audits	Current year + 6 years	Secure disposal

3. Pupil Records

Record Category	Retention Period
Pupil educational record	Date of birth + 25 years
Admissions register	Permanent archive review
Admissions appeals	Closure + 5 years
Unsuccessful admissions applications	End of admissions round + 1 year
Attendance records	Date of birth + 25 years
Examination results	Date of birth + 25 years
Behaviour records (routine)	Date of birth + 25 years (within pupil record)
Exclusion records	Date of birth + 25 years
Medical information impacting education	Date of birth + 25 years
Records relating to a child looked after by local authority	Date of birth + 75 years

4. Safeguarding

Record Category	Retention Period
Child protection records	Date of birth + 25 years
DSL chronologies	Date of birth + 25 years
Early Help records	Date of birth + 25 years
Online safety investigations	Date of birth + 25 years



Peer-on-peer abuse investigations	Date of birth + 25 years
Major safeguarding referrals	Date of birth + 25 years
Records relating to a child looked after by local authority	Date of birth +75 years
Records relating to children in need	Retain until the child is aged 25, or for 10 years after the case was received, whichever is longer

5. SEND

Record Category	Retention Period
SEND files	Date of birth + 25 years
EHC Plan documentation	Date of birth + 25 years
SEND reviews	Date of birth + 25 years
Specialist assessment reports	Date of birth + 25 years
Accessibility Strategy	Superseded + 6 years

6. Workforce

Record Category	Retention Period
Personnel file	Employment end + 6 years
Payroll records	Current year + 6 years
Recruitment records (unsuccessful)	6 months
DBS certificates	Up to 6 months
Single Central Record evidence	Employment end + 6 years
Occupational Health referrals	Employment end + 6 years
Sickness records	Employment end + 6 years
Flexible working requests	Closure + 18 months
Apprenticeship records	Completion + 6 years
Exit interviews	Employment end + 2 years
Capability records	Employment end + 6 years
Whistleblowing investigations	Closure + 6 years

7. Staff Safeguarding Allegations

Record Category	Retention Period
Staff safeguarding allegations	Until retirement age or 10 years from allegation, whichever longer
Malicious allegations	Remove from file once determination confirmed



8. Estates, Health & Safety

Record Category	Retention Period
Accident records (adult)	Incident + 6 years
Accident records (pupil)	Date of birth + 25 years
Fire risk assessments	Superseded + 6 years
Fire drill records	Current year + 6 years
Legionella records	5 years
Gas safety certificates	2 years
Electrical inspection certificates	Lifetime of certificate + 6 years
COSHH records	40 years
Asbestos records	Life of building + 40 years
Building condition surveys	Life of building + 6 years

9. Finance & Procurement

Record Category	Retention Period
Annual accounts	Current year + 6 years
Invoices	Current year + 6 years
Budget records	Current year + 6 years
Contracts under seal	Expiry + 12 years
Contracts under signature	Expiry + 6 years
Procurement documentation	Contract expiry + 6 years
Supplier due diligence	Contract expiry + 6 years

10. Digital Systems, Cyber Security and AI

Record Category	Retention Period
AI risk assessments	Life of system + 6 years
AI approvals	Life of system + 6 years
AI usage reviews	Current year + 6 years
AI incidents	Closure + 6 years
Supplier security assessments	Contract expiry + 6 years
Penetration tests	Current year + 6 years
Cyber incident investigations	Closure + 6 years
Access reviews	Current year + 3 years
System implementation records	Life of system + 6 years
Data migration records	Completion + 6 years



11. Biometrics, CCTV and Media

Record Category	Retention Period
Biometric templates	While actively required or pupil remains enrolled, then delete within 1 month
Biometric objections/consent records	Duration of use + 6 years
Routine CCTV footage	30-90 days
CCTV linked to investigation	Case closure + 6 years
CCTV disclosure logs	6 years
Marketing photographs	In line with consent or until withdrawn
Website and social media content	Review annually

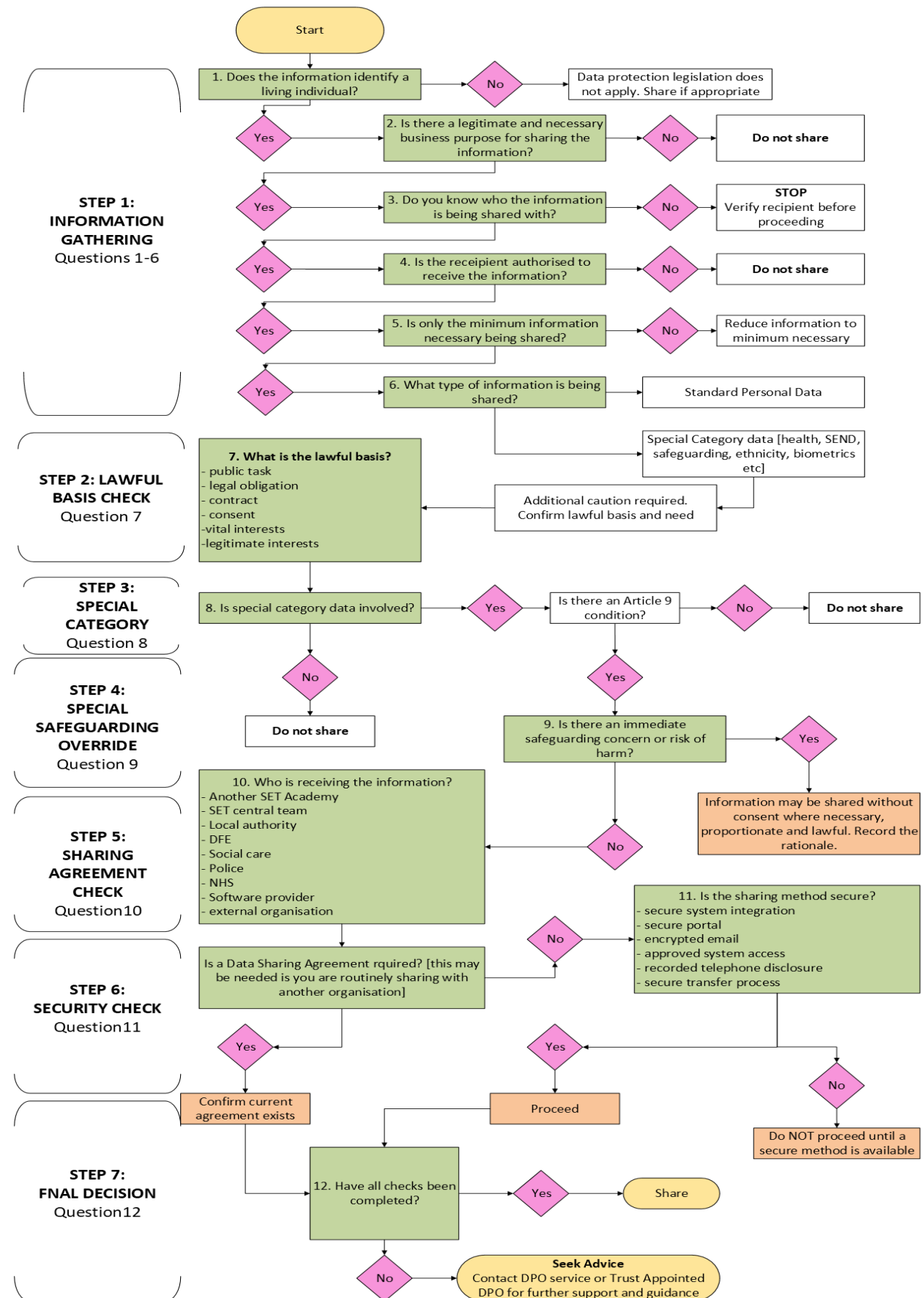
12. Permanent Archive Records

Some documents may be classified as permanent preservation items. These could include Articles of association, school historical records, historic photographs, major building projects, and Trust anniversary publications.

For any queries regarding the retention of data not mentioned within this guidance, please refer to the related Trust policy for further information. Where additional information is not found in the policy document, please contact the Trust Appointed DPO for further information.



Appendix K – Data Sharing Decision Tree





Appendix L – New Software and Online Platform Procurement/Adoption Protocol

Document type:	Procedural guidance
Owner:	Director of Data Strategy and Information Systems
Applicable to:	All academies and central teams
Review Frequency:	Annual [Aligned with DfE and Academy Trust Handbook Updates]

1. Purpose and core alignment

This protocol serves as a mandatory operational supplement to Section 10 (Data sharing, processors, and suppliers) and Section 12 (DPIAs and privacy by design) of the Shaw Education Trust Data Protection Policy 2026. Before any academy or central team adopts, purchases, or runs a free trial of any educational technology (EdTech), cloud computing system, software application, or online platform, they must complete the due diligence steps outlined below.

2. Purpose and core alignment

As established under the Trust's centralised data protection framework, ultimate accountability sits with the Trust Board. Operational management and sign-off are routed through a tiered approval structure to ensure compliance before any digital system processing data goes live.

Level	Authorised	Risk & Cost	Type of Data	Entry on ROPA
Level 1	Headteacher / DPL	Low risk, Low cost	No PII / Special Category	No entry
Level 2	DDIS	Medium risk, or Cost	Handles Pupils or Staff PII	Entry required
Level 3	DDIS	High risk, or high cost	Core trust wide system	Entry required

**DDIS = Director of Data and Information Systems*

**PII = Personally Identifiable Information*

The Academy appointed Senior Data Protection Lead will be consulted prior to the adoption of any new systems and will be jointly responsible, with the Headteacher, for adhering to the due diligence processes outlined within this document.



3. Mandatory Information Security Standards

To comply with Section 15 of the Data Protection Policy (Information Security and Cloud Computing) as well as our Data security Policy and Trust Wide Digital Strategy, any platform considered for procurement must pass these minimum technical safeguards.

Microsoft Single Sign-On (SSO): The platform must integrate natively with the central Trust identity infrastructure (Microsoft 365). Staff and students must authenticate using their existing Trust Microsoft credentials. Local password creation is strictly prohibited.

Multi-Factor Authentication (MFA): The platform must support and enforce MFA for all staff accounts, routing through our central Microsoft authenticator rules.

Cyber Accreditations: Suppliers must hold a verified **Cyber Essentials Plus** or **ISO 27001** certification. For all Level 3 Applications, Cyber Essentials Plus is the minimum non-negotiable benchmark.

Secure Data Flows: Software must connect via secure, documented APIs. Manual insecure data CSV uploads and downloads are forbidden as they introduce high breach risks.

4. Statutory Compliance and Risk Assessments

In line with section 12 of the main policy, data protection due diligence must take place **before** a tool is selected or trialled.

A Data Protection Impact Assessment is a mandatory requirement for high-risk processing, including systems handling large-scale pupil or staff data, biometrics, or AI features. Suppliers must confirm that all personal data is physically hosted within the **United Kingdom (UK)** or the **European Economic Area (EEA)**. Any international transfers must be escalated to the DPO service.

Any contracts must state that the supplier will securely delete all Trust data within 30 days of contract termination, aligned with our Trust Data Retention Schedule.

The safeguarding of all pupils will be considered if a student-facing platform allows interaction or content creation, any platform must align with the KCSIE standards. Any such system must not rely on simple keyword blocking; the system must actively flag concerning behavioural or safety patterns directly to the schools' Designated Safeguarding lead [DSL].



5. Commercial Rules and DfE Frameworks

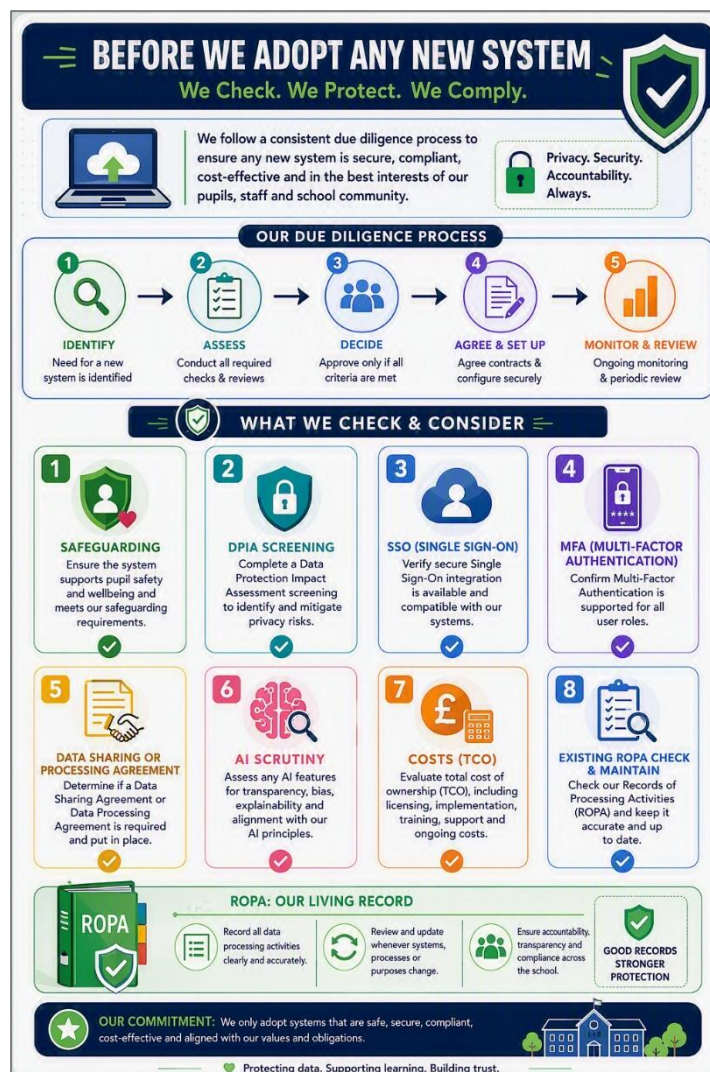
Schools must record total costs of ownership (TCO) and must itemise all hidden costs, including set up fees, integration fees, mandatory training, and projected year-on-year price increases.

For all Management Information Systems (MIS) procurement, the Trust will use the official DfE framework. Core contracts will be capped at a maximum of 3 years, and transitional extensions are limited to a maximum of 12 months.

6. Procurement Process

All schools and central teams will follow a process of due diligence and approval prior to the purchase or free trial of any new system.

When considering a new system, it is important all aspects of safeguarding, security and legislative compliance are considered. Further detailed information has been laid out within supplementary documents associated with this policy.





7. Artificial Intelligence (AI) Due Diligence Checklist

If the platform utilises any form of generative AI, Machine Learning, or Large Language Models (LLMs), the supplier must meet the DfE product safety standards and the expectations of the Trust-wide AI strategy.

No.	Due Diligence Area	Mandated Criteria / Trust Requirement	Supplier Confirmation / Evidence
1	Model Training & Privacy	The vendor must legally guarantee that our pupil data, staff data, and uploaded schoolwork will not be used to train their AI models.	
2	Content Guardrails	The vendor must provide proof of automated content filters that prevent students from encountering harmful, inappropriate, or biased AI outputs.	
3	Human Review Control	The platform must allow teachers to override AI decisions. AI tools must not independently make significant decisions regarding student outcomes or behaviour sanctions.	
4	Data Entry Restrictions	Supplier confirms clear notices inside the app warning users not to input unapproved personal data, safeguarding info, or confidential Trust files.	

**The above has been extracted from the DfE AI national guidance*

See additional resources in conjunction with this document.

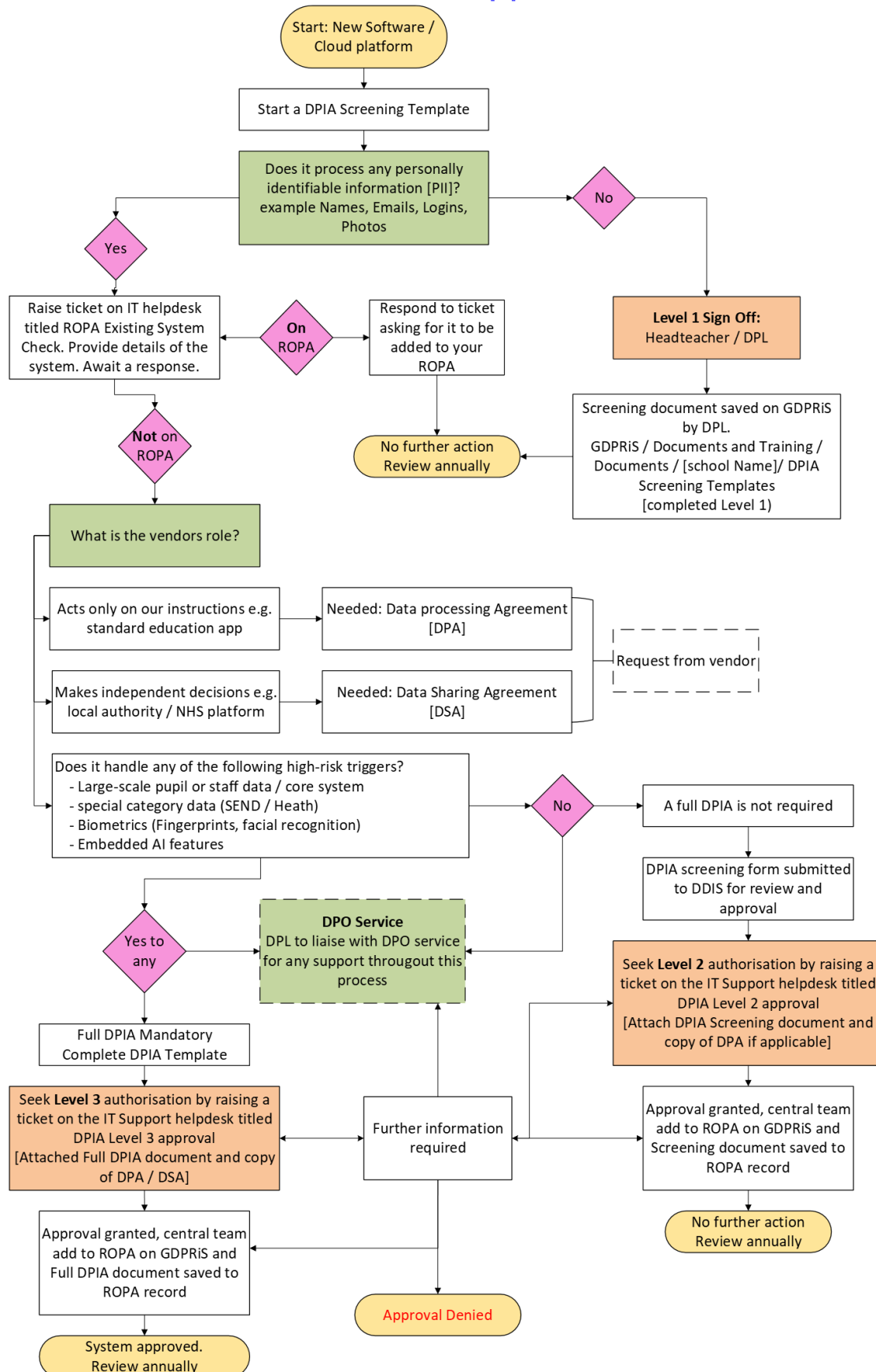
Appendix M - Software and Online Platform Procurement/Adoption -Flowchart

Appendix N - DPIA Screening Template: New Software & Digital Platforms

Appendix O - Data Protection Impact Assessment (DPIA) Template



Appendix M – Software and Online Platform Approval -Flowchart





Appendix N – DPIA Screening Template: New Software & Digital Platforms

Instructions for Project Lead: Complete Section 1 and Section 2, then forward this form to your Academy Data Protection Lead (DPL) before purchasing or starting a trial.

SECTION 1: System and Administrative Overview

School name:	
Form completed by [name & role]	
Name of proposed software / cloud Platform	
Include the URL of this provider or website	
Provide a brief description of what the software does:	
Target user group:	☐ Pupils / ☐ Teaching staff / ☐ Support staff / ☐ Parents

SECTION 2: High-Risk Trigger Assessment

Select **YES** or **NO** for each of the following questions based on the systems handling of data.

No.	High-risk Data Trigger Question	YES	NO
1	Large-Scale Processing / Core System: Will this platform be used across the whole school, multiple year groups, or trust-wide to manage core data (e.g., a new MIS, parent app, or central finance package)?	☐	☐
2	Special Category Data: Will the platform store or track sensitive info, such as pupil health conditions, allergies, SEND records, EHCP documents, or ethnic origin?	☐	☐
3	Biometric Technology: Will the system use physical data like fingerprints, finger geometry, or facial recognition scans for identification (e.g., cashless catering or library check-ins)?	☐	☐
4	Artificial Intelligence (AI): Does the tool use embedded AI, machine learning, or automated decision-making features to evaluate student work or track patterns?	☐	☐



5	Safeguarding & Online Monitoring: Will the platform track student online behaviour, web filtering logs, or store child protection chronologies/DSL files?	☐	☐
6	Location Tracking: Will the application track the real-time physical location of pupils or staff (e.g., school trip trackers or bus apps)?	☐	☐

SECTION 3: Academy DPL Review and Decision

To be completed by the Academy DPL after reviewing Sections 1 and 2.

☐ Outcome A: Level 1 approval only	<u>Trigger:</u> All answers in Section 2 were “No”. <u>Action:</u> A full DPIA is not required. File this signed DPIA screening template form on GDPRiS as per the process. Ensure a Data Processing Agreement (DPA) is in place, and add the platform
☐ Outcome B: Level 2 approval required	<u>Trigger:</u> Personally, Identifiable Information will be shared, or DPO service recommends completing a DPIA. <u>Action:</u> A full DPIA may not be required. Share this DPIA screening template for review centrally by the DPO.
☐ Outcome C: Level 3 approval required	<u>Trigger:</u> At least one “Yes” was ticked in Section 2. <u>Action:</u> Stop procurement. The school must generate and submit a full DPIA template for review and approval centrally by the DPO.
Academy DPL Signature	
Date signed	

Refer to the Trust Data Protection Policy for guidance on the correct processes to follow.
Appendix M - Software and Online Platform Approval -Flowchart

SECTION 4: Trust Level Sign-Off (Level 2/ 3 Escalations)

To be completed by the Director of Data Strategy and Information Systems if the platform involves pupil/staff Personally Identifiable Information [PII].

IT Helpdesk Number:	
Decision:	☐ Approved ☐ Full DPIA form required
Signature (DDIS):	
Date:	



Appendix O – Data Protection Impact Assessment (DPIA) Template

This is a statutory template (aligned with Trust Data Protection Policy 2026 and ICO standards)

Instructions for Academy Data Protection Leads (DPL): Complete this full assessment for any system that triggered a “Yes” / Outcome C on the DPIA Screening template. Once completed, raise a ticket with the IT Helpdesk titled “**Level 3 DPIA Approval**” attaching this completed document, a copy of any relevant Data Sharing or Data processing Agreements and any other relevant information.

Please refer to the Data Protection Policy and Appendix M - Software and Online Platform Approval -Flowchart for further information regarding the process.

SECTION 1: Administrative and Project Overview

School name	
Academy Data Protection lead (DPL)	
Project lead / system owner	
Name of proposed software / cloud platform	
Estimated procurement costs (including any initial set up costs and minimum duration)	£ Min Duration:
Estimated go-live / deployment date	

SECTION 2: Description of the Processing

2.1 - Context and Data Flow

Why is this software required? What operational problem does it solve?

Whose data will the platform store or process? (select all that apply)

- ☐ Pupils ☐ Parents ☐ Teaching Staff ☐ Support Staff ☐ Volunteers or Governors
☐ Other Staff: _____



1.2 – Data Categories Checklist

Select all specific data items that will be uploaded to, or generated by, the platform.

Standard Personal Data (PII)	Special Category & Sensitive Data (High Risk)
☐ Full names / preferred names	☐ Child protection / Safeguarding
☐ School email addresses / logins	☐ SEND files, EHCPs, or learning specialist reports
☐ Home addresses or phone numbers	☐ Medical records, allergies, or health conditions
☐ Pupil admission / UPN numbers	☐ Biometric templates (fingerprints / facial recognition)
☐ Attendance and behaviour logs	☐ Real-time physical location / GPS tracking data
☐ Academic test results and target grades	☐ Racial, ethnic origin, or religious beliefs

SECTION 3: Lawfulness, Proportionality and Core Mandates

Verify that the platform adheres to our strict Trust operational boundaries.

3.1 Lawful basis: what is Academy / Trusts primary lawful basis for processing this data under UK GDPR Article 6? (ref Data Protection Policy Appendix K – Data Sharing Decision tree)

- ☐ Public Task (required for core education and school operations)
- ☐ Legal obligation (Required by statutory framework)
- ☐ Consent (Must be freely given, specific, auditable, and easy to withdraw)

3.2 Special category condition: If processing sensitive data, what Article 9 condition is met?

- ☐ Substantial public interest (Statutory / Governmental purposes)
- ☐ Employment, Social security, and Social Protection law
- ☐ Explicit consent



3.3 Data minimisation check: Can this platform operate successfully without uploading all data categories ticked above? Have you limited the data transfer to only what is strictly necessary? ☐ YES / ☐ NO

3.4 Identity infrastructure mandate: Does this platform natively support and enforce central Microsoft Single Sign-On (SSO) and Multi-factor Authentication (MFA) for all staff accounts? ☐ YES / ☐ NO

SECTION 4: Information Security and Supplier Due Diligence

To satisfy section 15 (Information Security and Cloud Computing) of the Data Protection Policy, confirm vendor standards.

4.1 Security accreditation: Confirm the vendors current security standard (attach proof)

☐ Cyber essentials plus ☐ ISO27001 ☐ Other: _____

4.2 Data hosting location: Where is the data physically stored by the provider?

☐ United Kingdom (UK) ☐ European Economic Area (EEA) ☐ Other: _____

4.3 Contractual compliance (DPA): Does the vendor agreement include a binding Data processing Agreement that guarantees full, secure data deletion within **30 days** of contract end? ☐ YES / ☐ NO

4.4 AI sub processor scrutiny (if applicable): Does the platform utilise embedded AI? If yes, does the vendor legally guarantee that our Trust data will **never** be used to train or fine-tune public models? ☐ YES / ☐ NO / ☐ N/A (No AI features)

SECTION 5: Risk Assessment / Reducing Risk

Identify the potential risks to the rights and freedoms of data subjects and details how the school will control them. The DPO service can support with a risk assessment.

Identified privacy risk / breach threat	Likelihood (Low/Med/High)	Impact (Low/Med/High)	Approved mitigation control / operational action	Resulting risk (Reduced or accepted)
<i>Example: Unauthorised access to sensitive student SEND files via local credential theft</i>	<i>Medium</i>	<i>High</i>	<i>Mandatory integration with Microsoft SSO and enforcement of staff MFA rules</i>	<i>Reduced to low</i>



Risk 1: Data breach or hacking attempt at the cloud vendor's data centre			Vendor holds active Cyber Essentials Plus certification and uses encrypted databases at rest.	
Risk 2: Insecure data transfers or data leakage during local imports/exports.			Manual CSV files are prohibited; system connects via an automated, secure system-to-system API.	
Risk 3: Vendor lock-in or data retention issues if the contract is terminated.			Contract contains a strict clause requiring complete data destruction within 30 days of exit.	
Risk 4:				
Risk 5:				

SECTION 6: Local Academy Sign-Off

"I confirm that the technical and operational details recorded within this assessment are accurate. This system will not go live, nor will any contract be finalised, until formal approval is logged centrally by the Trust."

DPL Signature:		Headteacher Signature:	
Date:		Date:	

** This document can be signed by either the DPL or Headteacher, but preferably by both.*

SECTION 7: Central Trust Review & Approval

To be completed by the Trust DPO service and the Director of Data Strategy and Information Systems.

Trust DPO service advice / recommendations.



Final Executive Decision

☐ Approved	☐ Deferred	☐ Rejected
The system meets all Trust 2026 standards. The school may proceed to contract signature	Additional vendor evidence or risk mitigation needed (see notes below)	This platform violates Trust security standards and compliance policies and cannot be adopted.
Director Signature		
Date form completed / closed:		





Appendix P – Consent Form – Parent for Event [2026]

(Use of Pupil Information, Images and Videos)

Name of pupil: _____ Pupils Form/Class: _____

Name of Event: _____ Date of Event: _____

Dear Parent / Carer,

We are writing to request your consent for the Academy, as part of Shaw Education Trust, to use your child's name, image, and/or video in connection with the above-named event.

We are proud to celebrate the achievements and activities of our pupils and may wish to use images or videos to promote these opportunities across our publications, website, and social media. We only use such materials when we have your explicit permission.

Under UK data protection law, including the UK GDPR and the Data Protection Act 2018 (as amended), we require parental consent to use the personal data of children aged 12 and under for these purposes. From age 13, young people may provide their own consent if they are able to understand what it means.

There is no obligation to give consent. Your decision will not affect your child's education or any services they receive. If you choose not to give consent, we will ensure your child is not identifiable in any materials created for the purposes you decline.

This consent applies only to the event specified in this form.

You may withdraw your consent at any time by contacting our Data Protection Officer (details provided below). When consent is withdrawn, we will stop using the material going forward, although we may retain copies for lawful purposes.

For further information on how we process personal data, your rights, and our retention practices, please read our Privacy Notices, available at: [insert school website link]

If you have any questions, please contact:

In School Data Protection Lead	
Email	
Telephone	

Yours Sincerely
[Principal Name]



Consent Form – Parent for Event [2026]

(Use of Pupil Information, Images and Videos)

Providing your consent

Please indicate Yes or No for each processing purpose. We will only use your child's information in ways for which you have given explicit consent.

I provide consent to:	Yes	No
Section A: School & Trust Websites		
– Use of my child's name on the school or Trust website in relation to the event.		
– Use of photos of my child on the school or Trust website. (Names will not be included without additional consent if the child is aged 12 or under.)		
– Use of videos of my child on the school or Trust website.		
Section B: Printed & Digital Marketing Materials		
– Use of photos of my child in printed or digital marketing materials (e.g., newsletters, Trust publications, promotional brochures).		
Section C: Social Media Platforms – <i>Please note: each platform may store data outside the UK. Appropriate safeguards will be applied.)</i>		
– Photos of my child on social media (e.g., Twitter/X, Facebook, Instagram, YouTube) in relation to the event.		
– Videos of my child on social media in relation to the event.		
Section D: External Media Outlets – <i>(Includes newspapers, sector publications, and online media. Content may be hosted outside UK.)</i>		
– Photos of my child used by approved media organisations to publicise the event or school/Trust activities.		
– Videos of my child used by approved media organisations to publicise the event or school/Trust activities.		

Parent/Carer Declaration

I, _____ (parent/carers name), confirm that I have read and understood the information provided in this form and the linked Privacy Notice. I understand that I may withdraw consent at any time by contacting the Data Protection Officer.

Signature: _____ Date: ____/____/____

Notes on Your Rights

- You can withdraw any consent you have given, at any time, without affecting your child's education.



- No automated decision-making or profiling will be carried out using your child's images or videos.
- We apply appropriate data protection safeguards whenever material may be transferred or accessed outside the UK.



Appendix Q – Consent Form – Parent General [2026]

Pupil Image & Information Consent Form (Parent/Carer)

Dear Parent/Carer,

We are writing to request your consent for **[Academy Name]**, part of Shaw Education Trust, to use your child's name, photograph, and/or video in connection with a range of school and Trust activities.

We are proud of the achievements of our pupils and may wish to use images or videos to promote these activities through our website, printed materials, social media, and communications with the wider community. We will only use your child's information for the activities for which you give explicit consent.

Under UK data protection law, including the UK GDPR and the Data Protection Act 2018 (as amended by the Data Use and Access Act 2025), parental consent is required for **pupils aged 12 and under**. From **age 13**, pupils may choose to give their own consent where they can understand what it means.

You are under **no obligation** to give consent. If you decline consent for any category, your child will not be identifiable in materials created for those purposes. This will not affect their education or access to school activities.

This consent applies only to the uses listed below. **You may withdraw your consent at any time** by contacting our Data Protection Lead (details below). When consent is withdrawn, we will stop using the material, although we may retain copies for lawful reasons (e.g., educational records). Please note that a head and shoulders photo of your child will be retained for identification and safeguarding purposes and stored securely within our management information system within their educational record.

It is our policy to annually review this data with you, we may ask you to review your consent part way through the year should the school or trust agree to adopt the use of any new platforms.

For further information on how we process personal data, your rights, and our retention practices, please read our Privacy Notices, available at: **[insert school website link]**

If you have any questions, please contact:

In School Data Protection Lead	
Email	
Telephone	

Yours Sincerely
[Principal Name]



Consent Form – Parent General [2026]

Pupil Image & Information Consent Form (Parent/Carer)

NAME OF PUPIL: _____ Pupils Class / Form: _____

Providing your consent

Please tick Yes or No for each option. We will only use your child's information for uses where you select Yes.

I provide consent to:	Yes	No
Section A: School & Trust Websites		
– Use of my child's name on the school or Trust website in relation to the event.		
– Use of photos of my child on the school or Trust website. (Names will not be included without additional consent if the child is aged 12 or under.)		
– Use of videos of my child on the school or Trust website.		
Section B: Printed & Digital Marketing Materials		
– Use of photos of my child in printed or digital marketing materials (e.g., newsletters, Trust publications, promotional brochures).		
Section C: Social Media Platforms – Please note: each platform may store data outside the UK. Appropriate safeguards will be applied.)		
– Photos of my child on social media (e.g., Twitter/X, Facebook, Instagram, YouTube) in relation to the event.		
– Videos of my child on social media in relation to the event.		
Section D: External Media Outlets – (Includes newspapers, sector publications, and online media. Content may be hosted outside UK.)		
– Photos of my child used by approved media organisations to publicise the event or school/Trust activities.		
– Videos of my child used by approved media organisations to publicise the event or school/Trust activities.		
Section E: Use After Child Leaves the School		
– Continued use of my child's approved images/videos after they leave the school (e.g., in prospectus or historical reflections).		

Parent/Carer Declaration

I confirm that I have read and understood the information provided in this form and the Academy's Privacy Notice. I understand that I may withdraw consent at any time by contacting the designated in school Data Protection Lead.

Name of parent / carer: _____

Signature: _____ Date: __ / __ / ____



Appendix R – Consent Form – Pupil (Age 13+)

Pupil Image & Information Consent Form (Parent/Carer)

(Use of Pupil Information, Images and Videos)

Name of pupil: _____ Pupils Form/Class: _____

Name of Event: _____ Date of Event: _____

Dear Student,

We would like to ask for your consent to use your name, photograph, and/or video in connection with the above-mentioned event.

The Academy, as part of Shaw Education Trust, is proud of the achievements of our pupils and the opportunities available across the Trust. With your permission, we may use images or videos of you to help promote these activities in our marketing materials, on our website, and on social media.

Because you are aged 13 or over, UK data protection law says you can make this decision yourself if you understand what it means. You do not have to give consent, and saying no will not affect your education, your opportunities in school, or any support you receive.

This consent applies only to the event named in this form.

You may withdraw your consent at any time by contacting our Data Protection Officer. When you withdraw consent, we will stop using your images from that point forward, although we may keep existing copies for lawful reasons (for example, educational record-keeping).

For further information on how we process personal data, your rights, and our retention practices, please read our Privacy Notices, available at: **[insert school website link]**

If you have any questions, please contact:

In School Data Protection Lead	
Email	
Telephone	

Yours Sincerely

[Principal Name]



Consent Form – Pupil (Age 13+)

Pupil Image & Information Consent Form (Parent/Carer)

(Use of Pupil Information, Images and Videos)

Providing your consent

Please read each statement carefully. Tick **Yes** if you agree to the use of your information for that purpose, or **No** if you do not agree. We will only use your information for the options where you say Yes.

I provide consent to:	Yes	No
Section A: School & Trust Websites		
– Using my name		
– Using my photo on the school or Trust website		
– Using video of me on the school or Trust website		
Section B: Printed & Digital Marketing Materials		
– Using my photo in any printed or digital marketing materials		
Section C: Social Media Platforms – (Please note: each platform may store data outside the UK. Appropriate safeguards will be applied.)		
– Using my photo on social media (e.g., Twitter/X, Facebook, Instagram, YouTube) in relation to the event.		
– Using video of me on social media in relation to the event.		
Section D: External Media Outlets – (Includes newspapers, sector publications, and online media. Content may be hosted outside UK.)		
– Use of my photo by approved media organisations to publicise the event or school/Trust activities.		
– Using video of me by approved media organisations to publicise the event or school/Trust activities.		

Pupil Declaration

I, _____, confirm that:

- I have read and understood the information in this form.
- I understand that I may withdraw consent at any time by contacting the Data Protection Officer.
- I have chosen **Yes** or **No** for each option, and the Academy will only use my information for the purposes I agree to.

Pupil Signature: _____ Date: ____/____/____



Appendix S – Privacy Notice for Pupils and Parents/Carers

Academic Year 2026-2027

1. Introduction

Shaw Education Trust ("the Trust") is committed to protecting the privacy and security of personal information. This Privacy Notice explains:

- What personal information we collect.
- Why we collect and use it.
- How we protect it.
- Who we share it with.
- How long we keep it.
- Your rights under UK data protection legislation.

Shaw Education Trust is the Data Controller for the personal information processed by its academies and central services unless otherwise stated.

2. Contact Details

The Data Controller is:

Shaw Education Trust,
Kidsgrove Secondary School,
Gloucester Road,
Kidsgrove,
Staffordshire.
ST7 4DL

If you have a question about how personal information is used or would like to exercise your information rights, please contact your schools Data Protection Lead in the first instance. They will be able to assist with most enquiries and, where appropriate, liaise with the Trust's Data Protection Officer.

Individuals may also contact the Trust's Data Protection Officer by emailing a request into info@shaw-education.org.uk

3. What Information Do We Collect?

We collect and process a range of information about pupils and, where relevant, parents and carers. This may include:

Personal Information	Pupil Characteristics
• Name • Date of birth • Gender	• Ethnicity • Nationality • Country of birth



• Address • Contact details • Unique Pupil Number (UPN) • Parent and emergency contacts • Parent National Insurance numbers (for FSM eligibility checking) • Unique Learner Number 14+years)	• Language information • Free School Meal eligibility • Pupil Premium eligibility
Educational Records • Attendance records • Assessment results • Progress information • Behaviour records • Exclusion information • Examination entries and results	SEND Information • Special Educational Needs records • Education, Health, and Care Plans (EHCPs) • Specialist assessments • SEND provision information
Safeguarding and Welfare Information • Pastoral information • Child protection records • Welfare concerns • Professional involvement and referrals	Medical Information • Medical conditions • Allergies • Dietary requirements • Medication records • Healthcare plans
Digital Services and Security Records • User account information • Educational platform usage • Device and network access records • CCTV images where applicable	Images and Media • Photographs • Video recordings • Identification images
Biometric Information Where an academy operates biometric systems, such as cashless catering, biometric information may be processed subject to appropriate legal safeguards, parental notification, and pupil rights. Alternative arrangements will always be available for pupils who do not participate.	
Nursery Provision Where an academy provides nursery provision, in addition, these academies may process, early years funding information, development checks, and early years assessments.	
Sixth Form / Post 16 Where an academy provides post 16 provision, in addition, these academies may process, youth support, careers advice, UCAS data, and post 16 funding data.	



4. Why We Collect and Use Information

We collect and use personal information to:

- Support teaching and learning.
- Monitor educational progress and attainment.
- Provide pastoral care and wellbeing support.
- Safeguard pupils.
- Manage attendance.
- Administer admissions and appeals.
- Support SEND provision.
- Communicate with parents and carers.
- Organise educational visits and enrichment activities.
- Meet legal and regulatory requirements.
- Maintain site security and pupil safety.
- Operate educational technology systems.
- Respond to complaints, concerns, and investigations.
- Manage legal and insurance matters where required.
- Manage examinations and qualifications.

5. What Law Allows Us to Use This Information?

Under UK GDPR and the Data Protection Act 2018, we process personal information using one or more of the following lawful bases: Legal Obligation, Vital Interests, Public Task, or Consent, where appropriate. Where special category information is processed, such as health, safeguarding, SEND, or ethnicity information, we apply an additional lawful condition permitted under data protection legislation.

The Trust has access to specialist DPO support services and will seek advice and guidance, as necessary.

6. Artificial Intelligence (AI) and Educational Technology

The Trust uses a range of approved educational technology platforms and digital systems to support education, safeguarding, communication, and administration. The Trust may also use approved artificial intelligence (AI) tools where appropriate.

Before new AI or educational technology systems are introduced, the Trust undertakes data protection and information governance assessments to ensure information is used safely and lawfully. AI systems will not make significant decisions about pupils without meaningful human review and oversight. Personal data must not be processed through unapproved AI systems.

7. CCTV

Many Trust academies operate CCTV systems to:

- Protect pupils, staff, and visitors.





- Safeguard individuals.
- Prevent and detect crime.
- Protect Trust property.

CCTV is used lawfully, proportionately, and securely. Further information can be found within the Trust CCTV Policy.

8. How Long Do We Keep Information?

The Trust retains information in accordance with its Data Retention Schedule.

Most pupil educational records are retained until the pupil reaches approximately 25 years of age, although some information may be retained for shorter or longer periods depending upon legal, safeguarding, or operational requirements.

Information is securely deleted, anonymised or archived when no longer required.

9. Who Do We Share Information With?

Where lawful and necessary, we may share information with:

- Parents and carers.
- Schools and colleges attended after leaving us.
- Local Authorities.
- The Department for Education (DfE).
- Examination and awarding bodies.
- Children's Services.
- Health professionals.
- Educational psychologists.
- Education Welfare Services.
- Police and law enforcement agencies.
- Courts and tribunals.
- Approved software and cloud service providers.
- Professional advisers, legal representatives, and insurers.
- Shaw Education Trust central teams that support academy operations.

We only share the minimum personal information necessary for the purpose concerned.

10. Why We Share Information

We do not share pupil information without a lawful basis. We are required by law to provide certain information to organisations such as the Department for Education and Local Authorities. These statutory data collections support School funding, educational policy, School accountability, and National research and statistics.

Further information regarding school data collections can be found on the GOV.UK website.



11. The National Pupil Database

The National Pupil Database (NPD) is owned and managed by the Department for Education. It contains information about pupils in schools in England and is used for:

- Educational research.
- Statistical analysis.
- Policy development.
- School improvement.

The Trust is legally required to provide information to the DfE through statutory collections such as the School Census. Some of this information is stored within the NPD. The DfE may share NPD information with organisations carrying out approved research, analysis, and statistical work under strict controls. Further information is available from the Department for Education.

12. Additional Information for Pupils Aged 13+

For pupils aged 13 and above, information may be shared with Local Authorities and youth support services where required by legislation to support education, training, and careers services.

Parents may request that only a limited set of information is shared before the pupil reaches the age at which those rights transfer to them.

13. Your Information Rights

Under UK GDPR, pupils and parents may have rights to:

- Access personal information.
- Correct inaccurate information.
- Restrict processing.
- Object to processing.
- Erase information in certain circumstances.
- Data portability where applicable.
- Withdraw consent where consent has been relied upon.
- Challenge decisions based solely on automated processing.

14. Subject Access Requests

Individuals may request access to personal information held by the Trust through a Subject Access Request (SAR).

For secondary-aged pupils aged 13+ years, the Trust will normally consider whether a pupil has sufficient maturity to exercise their own information rights. This assessment is made on a case-by-case basis.



For further information or to raise a request, pupils or parents should contact the school Data Protection Lead who can provide information regarding the process. The Trust will normally respond within one calendar month.

15. Complaints

If you have concerns about how your personal information is being used, please contact your schools Data Protection Lead in the first instance. If you feel the support you have been given has been unsatisfactory you may escalate your concerns for the attention of the Data Protection Officer at The Trust.

You also have the right to complain to the Information Commissioners Office (ICO).

Further information can be found via the ICO website.

16. Review

This document will be reviewed on an ongoing basis in line with any national changes to legislation and, as a minimum, on an annual basis.



Appendix T – Workforce Privacy Notice

For the attention of: Employees, Apprentices, Agency Staff, Volunteers, Casual workers
Academic Year 2026-2027

1. Introduction

Shaw Education Trust ("the Trust") is committed to protecting the privacy and security of workforce information. This privacy notice explains:

- What personal information we collect.
- Why we collect and use it.
- How we protect it.
- Who we share it with.
- How long we keep it.
- Your rights under data protection legislation.

This notice should be read alongside the Trust's:

- Data Protection Policy
- Information Asset and Retention Schedule
- Information Security Policy
- Data Breach Response Procedure
- Acceptable Use Policy

The Trust's information governance framework has been designed to meet the requirements of UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018, Data (Use and Access) Act 2025 and Employment, education, and safeguarding legislation applicable to academy trusts.

This notice applies to all employees, apprentices, casual workers, agency workers, and volunteers. Shaw Education Trust is the Data Controller for personal information processed by academies and central services.

2. Contacting Us

The Data Controller is:

Shaw Education Trust,
Kidsgrove Secondary School,
Gloucester Road,
Kidsgrove,
Staffordshire.
ST7 4DL

If you have questions about how your personal information is used, or wish to exercise your information rights, please contact your academy or department Data Protection Lead in the first instance.

Where appropriate, matters will be referred to the Trust's Data Protection Officer.



3. Information Governance and Accountability

The Trust is committed to demonstrating accountability for how workforce information is managed and protected. To support this, the Trust maintains:

- Records of Processing Activities (ROPA)
- Data Protection Impact Assessments (DPIAs)
- Data sharing arrangements
- Information security controls
- Data retention and disposal arrangements
- Mandatory workforce training programmes on GDPR and Cyber Security
- Information governance assurance and audit activities

The Trust regularly reviews and audits its processing activities to ensure compliance with legislation, regulatory requirements, and good practice.

4. Information We Collect

Depending on your role and relationship with the Trust, we may process:

Personal Information • Name, address and contact details • Date of birth • National Insurance number • Employee identifiers • Emergency contact details • Bank account details • Pension information	Recruitment Information • Application forms • CVs and employment history • References • Interview notes • Identity verification documents • Qualification records • Right to work documentation
Employment Information • Contracts • Salary and payroll records • Working hours and attendance information • Annual leave records • Professional development records • Training records • Appraisals and performance information • Professional memberships	Health and Wellbeing Information • Occupational health records • Sickness absence information • Health and safety information • Fitness to work assessments • Reasonable adjustment records
Equality and Diversity Information • Ethnicity • Religion or belief • Disability status	Security and Technology Information • User account information • System access logs • Security audit information • Device records



• Sexual orientation (where voluntarily provided) • Equality monitoring information	• Network activity records • Building access records • CCTV footage where applicable
Images and Media • Staff photographs • Website and promotional images where appropriate	Criminal Offence Data Where legally permitted and necessary, we may process information relating to criminal convictions, cautions, and safeguarding checks.
Biometric Information Where an academy operates biometric systems, such as cashless catering, biometric information may be processed subject to appropriate legal safeguards, parental notification, and pupil rights. Alternative arrangements will always be available for pupils who do not participate.	

5. Why We Use Workforce Information

We process workforce information to:

- Recruit and appoint staff.
- Verify eligibility to work in the UK.
- Maintain safeguarding records.
- Meet statutory safeguarding obligations.
- Maintain the Single Central Record.
- Deliver employment contracts.
- Pay salaries and administer pensions.
- Manage absence, wellbeing, and occupational health.
- Support workforce planning.
- Conduct appraisals and performance management.
- Investigate complaints and concerns.
- Administer disciplinary and grievance processes.
- Meet legal, financial, and regulatory obligations.
- Protect Trust systems and information assets.
- Prevent fraud and misuse of Trust resources.
- Manage legal claims, audits, and insurance matters.

6. Safeguarding and Recruitment Checks

As part of safer recruitment and safeguarding duties, the Trust may undertake:

- Disclosure and Barring Service (DBS) checks
- Barred List checks
- Teacher prohibition checks
- Section 128 checks
- Overseas checks where applicable
- Qualification verification checks
- Right to work checks
- Identity verification checks





The Trust is legally required to maintain a Single Central Record and comply with safeguarding legislation and Keeping Children Safe in Education requirements.

7. Lawful Basis for Processing

The Trust processes workforce information under one or more of the following lawful bases:

- Performance of a contract
- Legal obligation
- Public task
- Vital interests
- Legitimate interests where appropriate
- Consent where required

The lawful basis used will depend upon the nature and purpose of the processing activity.

8. Special Category Information

The Trust may process special category personal information, including health information, occupational health reports, disability information, ethnicity, religion or belief, trade union membership, and equality monitoring information. Where this information is processed, the Trust relies upon an appropriate condition under Article 9 of UK GDPR and the Data Protection Act 2018. This information is used only where necessary to meet employment law obligations, support staff health and wellbeing, make reasonable workplace adjustments, manage sickness absence, promote equality of opportunity, fulfil health and safety responsibilities, and ensure compliance with statutory and regulatory requirements.

9. Criminal Conviction Information

The Trust may process criminal conviction and safeguarding information where legally permitted and necessary. This may include information obtained through DBS checks, Safeguarding investigations, Regulatory checks, and Information disclosed during employment

Such information is processed only where supported by an appropriate lawful basis and additional legal condition.

10. Artificial Intelligence (AI), Automated Processing, and Information Security

The Trust uses approved cloud services, digital platforms, and educational technology systems to support operational activities. The Trust may also use approved artificial intelligence (AI) tools to support administration, analysis, and service improvement.



Before introducing AI systems that process personal information, the Trust undertakes appropriate governance assessments including supplier due diligence and, where required, Data Protection Impact Assessments (DPIAs).

The Trust will not:

- Permit personal information to be entered into unapproved AI systems.
- Allow AI to independently make significant employment decisions.
- Use AI as the sole basis for decisions relating to recruitment, disciplinary action, capability proceedings, promotion, sickness management, performance management, or dismissal.

10. 1 Automated Decision-Making

The Trust does not ordinarily make decisions that produce legal or similarly significant effects solely through automated processing. Where automated processing is used to support decision-making, meaningful human review and oversight will always be maintained. Individuals have rights under UK GDPR relating to automated decision-making and profiling.

10. 2 Monitoring and Security Controls

To protect staff, pupils, systems and information assets, the Trust operates proportionate monitoring and security controls which may include:

- User account monitoring
- Security and audit logging
- Device management
- Network monitoring
- Building access controls
- Cyber security monitoring
- CCTV systems
- Information governance audits

Monitoring is undertaken only where lawful, proportionate, and necessary to meet safeguarding, security, compliance or operational requirements.

11. CCTV

Many Trust sites operate CCTV systems for safeguarding, site security, crime prevention and protection of staff, pupils and visitors. CCTV footage is used only where lawful, proportionate and necessary.

Further information can be found within the Trust CCTV Policy.

12. Who We Share Information With

Where lawful and necessary, information may be shared with:





- Department for Education (DfE)
- Education and Skills Funding Agency
- Teaching Regulation Agency
- Disclosure and Barring Service
- Local Authorities
- HM Revenue and Customs
- Teachers' Pension Scheme
- Local Government Pension Scheme
- Occupational Health providers
- Payroll providers
- HR providers
- Insurance providers
- Legal advisers
- Auditors
- Software and cloud service providers
- Police and law enforcement agencies
- Courts and regulators

Only the minimum amount of information necessary will be disclosed.

13. Department for Education Workforce Census

The Trust is legally required to submit workforce information to the Department for Education. This data supports workforce planning, educational research, statistical analysis, funding arrangements and school accountability.

Further information regarding workforce collections is available from the Department for Education.

14. International Data Transfers

Some approved systems and suppliers used by the Trust may store or process information outside the United Kingdom. Where international transfers occur, the Trust will ensure appropriate safeguards are in place to protect personal information and comply with UK GDPR requirements.

These safeguards may include adequacy regulations, international transfer agreements or other legally recognised protection mechanisms.

15. How Long We Keep Information

The Trust retains workforce information in accordance with its Data Retention Schedule.

Retention periods vary according to the information being processed and applicable legal requirements. When information is no longer required, it will be securely destroyed, anonymised or archived.

16. Your Rights

Under UK GDPR, you may have rights to:

- Access your personal information.
- Correct inaccurate information.
- Restrict processing.



- Object to processing.
- Request erasure in certain circumstances.
- Request portability where applicable.
- Withdraw consent where consent is relied upon.
- Challenge decisions based solely on automated processing.

You also have the right to:

- Complain to the Information Commissioner's Office (ICO).
- Request information about how automated processing may affect you.
- Be informed about significant changes to how your information is processed.

Requests should normally be directed to the academy or department Data Protection Lead in the first instance. The Trust will normally respond within one calendar month

17. Complaints

If you have concerns about how your personal information is being used, please contact the Trust in the first instance.

You have the right to complain to the Information Commissioner's Office (ICO). Information is available from the ICO website and helpline.

18. Changes to This Notice

The Trust may update this Privacy Notice periodically to reflect changes in legislation, guidance, systems or processing activities. As a minimum this document will be reviewed annually.

The latest version will always be published on the Trust website and academy websites.



Appendix U – Supplier and Contractor Privacy Notice

Academic Year 2026-2027

1. Introduction

Shaw Education Trust ("the Trust") is committed to protecting the privacy and security of supplier and contractor information. This privacy notice explains:

- What personal information we collect.
- Why we collect and use it.
- How we protect it.
- Who we share it with.
- How long we keep it.
- Your rights under data protection legislation.

This notice applies to:

- Suppliers
- Sole traders
- Contractors
- Consultants
- Service providers
- Professional advisers
- Temporary service providers
- Individuals acting on behalf of supplier organisations

This notice should be read alongside the Trust's:

- Data Protection Policy
- Information Security Policy
- Information Asset and Retention Schedule
- Data Breach Response Procedure
- Acceptable Use Policy

The Trust's information governance framework has been designed to meet the requirements of UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018, Data (Use and Access) Act 2025 and Procurement, finance and education legislation applicable to academy trusts.

Shaw Education Trust is the Data Controller for personal information processed by academies and central services.

2. Contacting Us

The Data Controller is:

Shaw Education Trust,
Kidsgrove Secondary School,
Gloucester Road,
Kidsgrove,
Staffordshire.
ST7 4DL



If you have any questions about how your personal information is used, please contact the relevant academy, procurement contact or central team in the first instance. Individuals may contact the Data Protection Officer directly at any time.

3. Information We Collect

Depending upon the nature of the services provided, the Trust may process:

Personal Information • Names • Business addresses • Email addresses • Telephone numbers • Job titles • Business contact details	Financial Information • Bank account details • Payment details • VAT registration information • Company registration information • Payment history
Contract Information • Contracts • Service agreements • Purchase orders • Tender submissions • Contract performance information • Procurement records	Due Diligence Information • DBS information where required • Safeguarding suitability information • Insurance certificates • Accreditation records • Compliance declarations • Financial standing information
Information Security Information • Supplier assurance questionnaires • Security certifications • Cyber security assurances • Data protection compliance records • Data processing agreements	Site Security Information • Visitor records • Building access information • CCTV footage where applicable • Contractor sign-in records
The Trust typically obtains this information directly from suppliers, contractors and service providers or through procurement, due diligence and contract management activities.	

4. Why We Use Supplier and Contractor Information

- Procure goods and services.
- Administer contracts.
- Pay suppliers and contractors.
- Manage supplier relationships.
- Conduct due diligence checks.
- Assess compliance and risk.
- Meet safeguarding obligations.
- Manage information security risks.
- Verify supplier suitability.
- Comply with legal and regulatory obligations.
- Respond to complaints, incidents and investigations.



- Support financial management, audit and governance activities.
- Prevent fraud and misuse of Trust resources.

5. Lawful Basis for Processing

The Trust processes supplier and contractor information under one or more of the following lawful bases:

- Performance of a contract.
- Legal obligation.
- Public task.
- Legitimate interests where appropriate.
- Consent where required.

The lawful basis used depends upon the specific processing activity being undertaken.

6. Supplier Due Diligence and Governance

Before engaging suppliers, contractors or service providers, the Trust may undertake due diligence activities to assess suitability, compliance and risk.

These checks may include:

- Financial assessments.
- Insurance verification.
- References and accreditation checks.
- Safeguarding suitability checks.
- Security and cyber assurance reviews.
- Data protection assessments.
- Regulatory compliance reviews.
- Supplier assurance questionnaires.

The extent of due diligence will depend upon the nature of the services being provided and the level of risk involved. This may be repeated periodically throughout the contractual relationship. This reflects the Trust's accountability obligations under its Information Governance Framework.

7. Artificial Intelligence, EdTech and Technology Providers

Where suppliers provide digital systems, cloud services, educational technology or artificial intelligence (AI) services, the Trust may assess:

- Data categories processed.
- Supplier controller or processor status.
- Sub-processor arrangements.
- Hosting locations.
- International data transfers.
- Information security controls.
- Data retention arrangements.
- Deletion and exit arrangements.
- Children's data protections.
- AI governance and oversight arrangements.



Suppliers may be required to complete additional due diligence and contractual requirements where personal data or AI services are involved.

8. CCTV, Visitor Management and Site Security

Trust sites operate security and access control measures to protect staff, pupils, visitors and property. This may include visitor sign-in systems, building access controls, CCTV systems and contractor access records.

Information will only be used where lawful, proportionate and necessary for security, safeguarding or operational purposes

9. Who We Share Information With

Where lawful and necessary, information may be shared with:

- Finance system providers.
- Banking providers.
- Auditors.
- HM Revenue and Customs.
- Department for Education.
- Education and Skills Funding Agency.
- Local Authorities.
- Insurance providers.
- Legal advisers.
- Regulatory authorities.
- Police and law enforcement agencies.
- Approved software and cloud service providers.

Only the minimum information necessary will be disclosed.

10. Information Security

The Trust maintains technical and organisational security measures designed to protect personal information against unauthorised access, loss, destruction or misuse.

These measures may include access controls, user authentication, security monitoring, audit logging, cyber security controls, encryption, secure disposal arrangements, and supplier security requirements.

The Trust reviews security arrangements regularly as part of its information governance and cyber security programmes

11. International Data Transfers

Some approved suppliers and service providers may store or process information outside the United Kingdom. Where international transfers occur, the Trust will ensure that appropriate safeguards are in place in accordance with UK GDPR requirements.

Such safeguards may include adequacy regulations, international transfer agreements or other legally recognised protection mechanisms.



12. How Long We Keep Information

The Trust retains supplier and contractor information in accordance with its Information Asset and Retention Schedule. Examples of records retained include:

- Contracts.
- Procurement documentation.
- Supplier due diligence records.
- Financial records.
- Supplier assurance records.
- Data processing agreements.

Information is retained only for as long as necessary to meet legal, financial, contractual, regulatory and audit requirements before being securely destroyed, anonymised or archived.

13. Your Rights

Under UK GDPR, individuals may have rights to:

- Access their personal information.
- Correct inaccurate information.
- Restrict processing.
- Object to processing.
- Request erasure in certain circumstances.
- Request portability where applicable.
- Withdraw consent where consent has been relied upon.
- Challenge certain processing activities.

Requests should normally be directed to the Trust in writing and will usually be responded to within one calendar month.

14. Complaints

If you have concerns about how your personal information is used, please contact the Trust in the first instance.

You also have the right to complain to the Information Commissioner's Office (ICO).

Information on how to make a complaint is available on the ICO website.



15. Changes to This Notice

The Trust may update this Privacy Notice from time to time to reflect changes in legislation, guidance, systems, procurement arrangements or processing activities. As a minimum this document will be reviewed annually.

The latest version will always be published on the Trust website.



Appendix V – Governance Role Privacy Notice

Trustees, Members and Academy Councillors
Academic Year 2026-2027

1. Introduction

Shaw Education Trust ("the Trust") is committed to protecting the privacy and security of personal information relating to individuals undertaking governance roles within the Trust.

- What personal information we collect.
- Why we collect and use it.
- How we protect it.
- Who we share it with.
- How long we keep it.
- Your rights under data protection legislation.

This notice applies to:

- Members of the Trust.
- Trustees.
- Academy Councillors.
- Individuals being considered or appointed to a governance role.
- Former governance role holders where the Trust continues to retain information about their appointment or service.

This notice should be read alongside the Trust's:

- Data Protection Policy
- Information Asset and Retention Schedule
- Information Security Policy
- Data Breach Response Procedure
- Acceptable Use Policy

The Trust's information governance framework has been designed to meet the requirements of UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018, Data (Use and Access) Act 2025 and Procurement, finance and education legislation applicable to academy trusts.

Shaw Education Trust is the Data Controller for personal information processed by academies and central services.

2. Contacting Us

The Data Controller is:

Shaw Education Trust,
Kidsgrove Secondary School,
Gloucester Road,
Kidsgrove,
Staffordshire.
ST7 4DL





If you have any questions about how your personal information is used, please contact the relevant academy, procurement contact or central team in the first instance. Individuals may contact the Data Protection Officer directly at any time.

3. Information We Collect

Depending upon your governance role, the Trust may process:

Personal Information • Name. • Previous names where required for regulatory checks. • Address. • Email address. • Telephone number. • Date of birth. • Photograph where applicable. • Emergency contact information where required.	Governance and Appointment Information • Governance role. • Date of appointment. • Term of office. • Date of resignation or cessation of office. • Method or basis of appointment. • Governance identification or reference numbers. • Committee and governance responsibilities. • Attendance at meetings. • Training and development records. • Skills, experience and professional background. • Relevant qualifications and professional memberships. • Correspondence relating to the governance role.
Statutory and Regulatory Information • Identity verification information. • Eligibility and disqualification checks. • Declaration of interests. • Pecuniary and business interests. • Relationships or interests requiring declaration. • Information required for statutory governance records. • Information required by the Department for Education or other regulatory bodies.	Safeguarding and Suitability Information Where required and legally permitted, this may include: • Disclosure and Barring Service information. • Section 128 checks. • Identity documents. • Suitability and eligibility declarations. • Information relating to restrictions or disqualification from governance.
Governance Activity The Trust may process information generated through governance activities, including:	Expenses and Financial Information Where applicable: • Bank details.



• Meeting attendance. • Contributions recorded within formal minutes. • Committee membership. • Decisions and approvals. • Declarations of interest made during meetings. • Governance correspondence. • Records relating to complaints, investigations or other governance matters.	• Expense claims. • Payment records. • Supporting receipts and financial documentation.
Information Security and Technology Where Trust systems or accounts are provided: • User account information. • System access records. • Security and audit logs. • Device information. • Cyber security and information governance training records.	Images and Site Security Where applicable: • Photographs used for governance or Trust communications. • Visitor records. • Building access information. • CCTV footage.

4. Why We Use Governance Information

The Trust may process governance information to:

- Appoint and maintain appropriate governance arrangements.
- Verify eligibility to undertake governance roles.
- Meet statutory and regulatory governance obligations.
- Maintain statutory registers and governance records.
- Administer Trust Board, committee and Academy Council activity.
- Manage meetings and governance communications.
- Record attendance, decisions and declarations of interest.
- Manage conflicts of interest.
- Publish information where required by law or regulatory requirements.
- Provide governance training and development.
- Maintain appropriate safeguarding arrangements.
- Support effective governance, scrutiny and accountability.
- Administer governance expenses where applicable.
- Manage complaints, concerns and investigations.
- Meet audit, assurance and regulatory requirements.
- Protect Trust systems, information and assets.
- Respond to legal proceedings or regulatory enquiries.



5. Lawful Basis for Processing

The Trust processes governance information under one or more lawful bases provided by UK GDPR, depending upon the activity. These may include:

- Legal obligation.
- Public task.
- Legitimate interests where appropriate.
- Performance of a contract or similar arrangement where applicable.
- Vital interests in limited circumstances.
- Consent where required.

The lawful basis used will depend upon the nature and purpose of the processing activity.

Where special category information or criminal offence information is processed, an appropriate additional condition will also be identified.

6. Special Category Information

The Trust may process special category personal information where this is necessary and lawful.

This may include information relating to:

- Health or disability.
- Racial or ethnic origin.
- Religious or philosophical beliefs.
- Trade union membership.
- Other special category information arising through equality monitoring or governance activities.

Such information will only be processed where necessary and where an appropriate condition under Article 9 UK GDPR and the Data Protection Act 2018 applies.

Access will be limited to those who require the information for an authorised purpose.

7. Criminal Conviction, Safeguarding and Eligibility Information

The Trust may process criminal conviction, safeguarding and eligibility information where legally permitted and necessary for the governance role.

This may include information obtained through:

- DBS checks.
- Section 128 checks.
- Governance eligibility and disqualification checks.



- Safeguarding investigations.
- Information disclosed during appointment or while undertaking the role.

Such information will only be processed where there is an appropriate lawful basis and additional legal condition.

The Trust's existing policy specifically requires trustees and academy councillors to protect personal data obtained through their governance duties.

8. Publication of Governance Information

Some information concerning individuals holding governance roles may need to be made publicly available to meet statutory, regulatory and transparency requirements.

This may include governance information published through:

- Trust or academy websites.
- Statutory governance registers.
- Department for Education systems and services.
- Other statutory or regulatory publications.

Only information required for the relevant purpose will be published.

9. Who We Share Information With

Where lawful and necessary, governance information may be shared with:

- Department for Education.
- Education and Skills Funding Agency.
- Companies House where applicable.
- Disclosure and Barring Service.
- Local Authorities where appropriate.
- Auditors.
- Legal advisers.
- Insurance providers.
- Governance support providers.
- Approved software and cloud service providers.
- Professional advisers.
- Regulatory authorities.
- Police and law enforcement agencies.
- Courts and tribunals where required.

Only the minimum amount of personal information necessary for the purpose will be disclosed.



10. Governance Papers, Minutes and Records

Trustees, Members and Academy Councillors may be identified within governance documents including agendas, minutes, committee papers, declarations of interest and decision records.

Some governance records form part of the Trust's permanent corporate record.

The Trust's Appendix J - Information Asset and Retention Schedule [2026] currently specifies permanent retention/archive for approved Trust Board minutes and Trust Board papers, permanent retention for committee minutes, and current year plus six years for committee papers. It also specifies retention requirements for governance reviews and complaints dealt with by trustees.

Information contained within governance records will be managed in accordance with the Trust's Information Asset and Retention Schedule.

11. Artificial Intelligence, Automated Processing and Information Security

The Trust may use approved digital services, cloud platforms and artificial intelligence tools to support administrative and governance activities.

Where AI or other technologies process personal information, appropriate governance arrangements will be applied, including risk assessment, supplier due diligence and Data Protection Impact Assessments where required.

Personal or confidential governance information must not be entered into unapproved AI systems.

The Trust does not ordinarily make decisions producing legal or similarly significant effects concerning governance role holders solely through automated processing.

Where Trust systems are provided to governance role holders, appropriate security measures may include:

- User authentication and access controls.
- Security and audit logging.
- Device management.
- Cyber security monitoring.
- Access reviews.

12. International Data Transfers

Some approved systems and suppliers used by the Trust may store or process information outside the United Kingdom.



Where international transfers occur, the Trust will ensure appropriate safeguards are in place to protect personal information and comply with UK GDPR requirements.

These may include adequacy regulations, international transfer agreements or other legally recognised safeguards.

13. How Long We Keep Information

Governance information is retained in accordance with the Trust's Information Asset and Retention Schedule.

Retention periods depend upon the type of record, statutory requirements and whether the information forms part of the Trust's permanent governance record.

For example, the Trust's current schedule provides for permanent archiving of approved Trust Board minutes, Trust Board papers and committee minutes, while other governance records have defined retention periods.

Where information is no longer required, it will be securely destroyed, anonymised or archived in accordance with the Trust's retention requirements.

14. Your Information Rights

Under UK GDPR, you may have rights to:

- Access your personal information.
- Correct inaccurate information.
- Restrict processing.
- Object to processing.
- Request erasure in certain circumstances.
- Request data portability where applicable.
- Withdraw consent where consent is relied upon.
- Challenge decisions based solely on automated processing.

These rights are not absolute, and their application will depend upon the circumstances and lawful basis for processing.

Requests should normally be directed to the Trust in the first instance. The Trust will normally respond within one calendar month, consistent with the approach taken in your existing privacy notices.

15. Complaints

If you have concerns about how your personal information is being used, please contact the Trust in the first instance.

You also have the right to complain to the Information Commissioner's Office (ICO).

Information about making a complaint is available from the ICO.



16. Changes to This Notice

The Trust may update this Privacy Notice periodically to reflect changes in legislation, guidance, governance arrangements, systems or processing activities.

As a minimum, this document will be reviewed annually. The latest version will be published through the appropriate Trust communication channels.

Opportunity



Integrity



Community



Equity



Working together to inspire communities where every school
is valued, every voice matters and every learner thrives.



**Shaw
Education
Trust**

Shaw Education Trust Head Office,
Kidsgrove Secondary School, Gloucester Road,
Kidsgrove, ST7 4DL

Email: info@shaw-education.org.uk

Call: 01782 948259

Visit: shaw-education.org.uk

LinkedIn: [@ShawEducationTrust](https://www.linkedin.com/company/ShawEducationTrust)