Data Protection Policy

Policy Type	Statutory Trust Policy
Author	Director of Operations
Approved By	Trust Board
Approved Date	September 2025
Date of next review	Annually
Version History	Version 2
Description of changes	Summary of changes outlined on Page 2

Policy Information:

Date of last review	September 2025	**Review period**	Annual
Date approved	23rd September 2025	**Approved by**	Trust Board
Policy owner	Director of Operations	**Date of next review**	September 2026

Updates made since the last review:

Review date	Changes made	By whom
September 2025	Insert school names - Section 1 Insert Data (Use and Access) Act 2025 - Section 3 Data Protection Law Amend Adequacy - Section 7 Management Policy - Section 9 Insert use of social media and messaging systems statement - Section 12 Amend AI statement - Section 12 Insert DUAA requirement for Official Bodies - Section 19	DPO

Contents

1 Introduction

Shine Academies Trust collects and uses the personal data of employees, pupils, parents, volunteers (including members of its governance structures) and other individuals. This information is gathered in order to enable the Trust to deliver teaching and learning, provide education services and discharge other associated functions. In addition, the Trust uses personal data in order to fulfil its statutory responsibilities as a Public Authority.

SHINE Academies Trust is registered with the Information Commissioner's Office: Registration Number ZA575317.

The Trust is recognised as a data controller, as it is the body responsible for determining how it uses personal data it collects, stores and shares.

All employees, volunteers and service providers of the Trust, or its schools (Busill Jones Primary School, Crowmoor Primary School, Lodge Farm Primary School, Martin Wilson Primary School, Northwood Park Primary School, Villers Primary School) are obliged to comply with this Policy when processing Personal Data on our behalf.

Failure by to comply with this policy carries the risk of significant civil and criminal sanctions for the individual and the Trust and may in some circumstances amount to a criminal offence by the individual. Any failure to comply with this policy may lead to disciplinary action under the Trust's procedures. The Information Commissioner's Office may also take action against individuals who willingly misuse or unlawfully process personal data that they are responsible for.

2 About this policy

The Trust holds Personal Data about current, past and prospective pupils, parents, employees and other individuals with whom the Trust communicates. Personal Data may be recorded on paper, stored electronically, visual media or other formats.

This Policy and other documents referred to in it set out the basis on which the Trust will process any Personal Data it collects from individuals, whether those data are provided to us by individuals or obtained from other sources. It sets out the expected data protection standards and the legal conditions that must be satisfied when we obtain, handle, disclose or transfer and store Personal Data.

This Policy does not form part of any employee's contract of employment and may be amended at any time.

The Data Protection Officer is responsible for supporting the Trust with compliance with the relevant Data Protection Laws and with this Policy. That post is held by Services4Schools Ltd.

Any questions about the operation of this Policy or any concerns that the Policy has not been followed, should be referred in the first instance to the Data Protection Officer. The Data Protection Officer can be contacted at DPO@shineacademies.co.uk

3 Definition of data protection terms

In this Policy, the functions of the Trust are the provision of education and any pastoral, business, administrative, community or similar activities associated with that provision. References to the Trust 'carrying out its functions' or similar are references to these activities. References to 'we' are references to the Trust and its schools.

Data Subjects means identified or identifiable natural (living) persons whose Personal Data is held by the Trust. These may be pupils, parents/carers, staff, governors, visitors etc. This Policy also refers to Data Subjects as 'individuals.'

Data Controllers are the people who, or organisations which, determine the purposes for which any Personal Data are processed, including the means of the processing. The Trust and its schools are the Data Controllers of all Personal Data used for carrying out its functions.

Trust Staff are, for the purposes of this Policy, those of our employees and volunteers (at Trust or school level) whose work involves processing Personal Data. Trust staff must protect the data they handle in accordance with this Policy and any applicable data security procedures at all times.

Data Processors include any person or organisation, who is not a member of Trust staff, which processes Personal Data on our behalf, including any external suppliers that handle Personal Data on the Trust's behalf.

Privacy Notices are documents explaining to Data Subjects how their data will be used by the Trust.

Personal Data means any information relating to an identified or identifiable natural (living) person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal Data Breach means the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data the Trust is responsible for.

Pseudonymisation means the processing of Personal Data so that it can no longer be attributed to a specific person without the use of additional information. This additional information (or key) must be kept separately and is subject to measures to ensure that the identity of the data subject remains protected.

Relevant Data Protection Law means the Data Protection Act 2018, the UK General Data Protection Regulation (UKGDPR), the Data (Use and Access) Act 2025, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426) and all applicable laws and regulations relating to the processing of Personal Data and privacy as amended, re-enacted, replaced or superseded from time to time and where applicable the guidance and codes of practice issued by the United Kingdom's Information Commissioner.

Special Categories of Personal Data (formerly known as 'sensitive Personal Data') include information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, sexual life and genetic or biological traits. Special Categories of Personal Data can only be processed under strict conditions.

4 Data protection principles

Anyone processing Personal Data for, or on behalf of, the Trust must comply with the principles of good practice contained in Relevant Data Protection Law. These principles state that Personal Data must be:

- processed fairly, lawfully and transparently;
- processed for specified, limited and legitimate purposes and in an appropriate way;
- adequate, relevant and not excessive for the purposes for which they are processed;
- accurate and, where necessary, kept up to date;
- not kept longer than necessary for the intended purpose of processing; and
- processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The Trust will keep a record of all data processing activities and must be able to demonstrate its compliance with these principles and with the wider requirements of Relevant Data Protection Law.

5 Fair, lawful and transparent processing

For Personal Data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in Relevant Data Protection Law. These include, but are not limited to:

- the individual's explicit consent to the processing for one or more specified purposes;
- that the processing is necessary for the performance of a contract with the individual or for the compliance with a legal obligation to which the Trust is subject;
- that the processing is in the public interest; or

- Where it is in the vital interests of an individual; or
- that the processing is in the legitimate interest of the Trust or relevant third parties to which the data are disclosed, so long as this is balanced with the rights and freedoms of the individual.

Where a change to a process, or introduction of a new process involving the use of large volumes of Data Processing, that is likely to pose a high risk to individuals' rights, the Trust will carry out a Data Privacy Impact Assessment in line with Article 35 of UKGDPR.

Special Categories of Personal Data

When Special Categories of Personal Data are being processed, the individual's explicit consent to processing of those data must be obtained unless the processing:

- is necessary for the purposes of carrying out the obligations and exercising specific rights of the Trust or of the individual in the field of employment and social security and social protection law;
- is necessary for the assessment of the working capacity of an individual where the individual is an employee or for the provision of health or social care;
- relates to Personal Data which are manifestly made public by the individual;
- is necessary for reasons of substantial public interest; or
- is necessary to protect the vital interests of the individual.

Processing of data relating to Criminal Convictions and Offences can only take place under control of an official authority, such as instructions from the police or an order of the court, or where law states that processing must take place.

This is undertaken as part of the pre-employment check process (DBS) for all staff employed by the Trust, or where it is necessary to perform such a check as required by safeguarding regulation.

Consent of adults and organisation

Where an individual gives consent to Data Processing, that consent must be freely given, specific, informed and unambiguous and should be either in the form of a statement (whether or not prepared by the Trust) or a positive action demonstrating consent. Any requests that the Trust makes for consent must be in clear language.

An individual has the right to withdraw consent at any time and will be informed of this right and how to exercise it when the Trust requests consent.

Consent of children and young people

Parental consent to Data Processing must be obtained for pupils or other children younger than 13 years of age.

6 Processing for Specified, limited and legitimate purposes

In the course of carrying out its functions, the Trust may collect and process the Personal Data set out in its data asset register. This may include data we receive directly from an individual (for example, by completing forms or by corresponding with us by post, phone, email or otherwise) and data we receive from other sources (including, for example, parents/carers, other schools, the local authority or other public bodies, previous employers, recruitment agencies or service providers, professional advisers and others).

The Trust will only process Personal Data for the specific purposes set out in Privacy Notices, or for any other purposes specifically permitted by Relevant Data Protection Law. We will explain those purposes to the Data Subject in Privacy Notices.

CCTV is used in some schools across the Trust to support the prevention and detection of crime, maintain site security, and to support pupil behaviour and safeguarding policies. Operation of CCTV systems installed at school sites must be undertaken in accordance with the Trust CCTV Policy and Procedure.

Where the use of CCTV includes the recording of images of identifiable individuals, the Trust will comply with the Data Processing principles within this Policy.

The Trust will adhere to the ICO's Code of Practice for the use of CCTV. All pupils, staff and visitors will be notified that CCTV is in operation via relevant signage.

The Trust will ensure that all CCTV footage will be kept for up to a maximum of 30 calendar days for security purposes before being deleted, unless the footage is exported for another purpose, for example where it required to support a criminal, or internal investigation.

Any enquiries about CCTV systems across the Trust should be directed to the Trust's Director of Operations.

7 Adequate, relevant and non-excessive processing

The processing of Personal Data will be limited to what is relevant and necessary to achieve the purposes set out in our Privacy Notices, or where this is a requirement if Relevant Data Protection Law.

All staff are required to adopt measures including data minimisation and pseudonymisation to limit the volume of personal data being processed by the Trust.

Staff are advised through training, policy and additional guidance of the need to ensure processing is necessary, relevant and consistent with the purposes defined in the Trust's Privacy Notices.

If a member of staff has any doubt as to whether any processing exceeds the purposes for which that data was originally collected, they should seek advice from the Data Protection Officer.

8 Accurate and up to date data

We will ensure that Personal Data we hold is accurate and kept up to date. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

Each school will be proactive in conducting regularly checks to validate the accuracy of the personal data they hold. This will include checking the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. Schools will also use the systems available to them to make personal data accessible to relevant individuals (parents and staff), so data accuracy can be checked directly by data subjects.

It is the responsibility of all staff to ensure that Personal Data is accurate and kept up to date. If staff become aware that personal data is incorrect or requires updating, they should make this change in school systems, or notify the relevant person who has access to make this change without delay.

All staff must as a minimum check that any Personal Data that they provide to the Trust in connection with their employment is accurate and up to date. They must also inform the Trust of any changes to their Personal Data that they have provided, e.g. change of address, either at the time of appointment or subsequently.

9 Timely processing

We will not keep Personal Data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which are no longer required. The Trust operates a Records Management Policy and Retention Schedule in respect of decision making concerning the retention of records containing Personal Data.

If a member of staff has any doubt as to whether any Personal Data has been or will be kept longer than is necessary for the purpose or purposes for which they were collected, they should notify the Data Protection Officer.

10 Processing Securely and in line with rights of Data Subjects

We are committed to upholding the rights of individuals provisioned to individuals under Relevant Data Protection Legislation.

We will process all Personal Data in line with individuals' rights, in particular their rights to:

a) be informed, in a manner which is concise, transparent, intelligible and easily accessible and written in clear and plain language, of the purpose, use, recipients and other processing issues relating to data;

b) receive confirmation as to whether your Personal Data is being processed by us;

c) access your Personal Data which we are processing only by formal written request. We may charge you for exercising this right if we are allowed to do so by Relevant Data Protection Law. Trust employees who receive a written request should forward it to their line managers and the Data Protection Officer immediately;

d) have data amended or deleted under certain circumstances where data is inaccurate or to have data completed where data is incomplete by providing a supplementary statement to the Trust

e) restrict processing of data if one of the following circumstances applies:

- the accuracy of the Personal Data is contested by the Data Subject, for a period enabling the controller to verify the accuracy of the Personal Data;
- the processing is unlawful and the Data Subject opposes the erasure of the Personal Data and requests the restriction of their use instead;
- the controller no longer needs the Personal Data for the purposes of the processing, but they are required by the Data Subject for the establishment, exercise or defence of legal claims;
- the Data Subject has objected to processing pending the verification whether the legitimate grounds of the controller override those of the Data Subject.

f) Where processing has been restricted, as above, such Personal Data shall, with the exception of storage, only be processed with the Data Subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest and the Data Subject shall be informed.

g) where processing is restricted, the data shall only be processed with the individual's consent or in relation to the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the or the United Kingdom;

h) an individual who has obtained restriction of processing shall be informed by the Trust before the restriction of processing is lifted;

i) receive data concerning the individual, which they have provided to the Trust and is processed by automated means, in a structured, commonly used and machine-readable format and to transmit those data to another controller without hindrance from the Trust;

j) object to Data Processing on grounds relating to his or her particular situation unless the Trust demonstrates compelling legitimate grounds for processing which overrides the interests, rights and freedoms of the individual or for to the establishment, exercise or defence of legal claims; and

k) not to be subject to a decision based solely on automated decision-making and profiling which produces legal effects concerning him or her or similarly significantly affects him or her unless the decision is based on the individual's explicit consent.

It is the responsibility of all staff to ensure that any request by an individual to exercise information rights is brought to the attention of the Data Protection Officer without undue delay.

The Trust may refuse a request by an individual wishing to exercise one of the above rights in accordance with Relevant Data Protection Law.

The Trust shall provide information on action taken on a request under paragraph to the individual within one month of receipt of the request unless the Trust deems it necessary to extend this period by two further months where the request is complex and informs the individual of such extension with reasons within one month of receipt of the request.

If a request is unfounded or excessive, the Trust may charge a reasonable fee for providing the information or refuse the request.

When receiving telephone enquiries, we will only disclose Personal Data we hold on our systems if the following conditions are met:

- We will check the caller's identity to make sure that information is only given to a person who is entitled to it.
- We will suggest that the caller put his or her request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

Our employees will refer a request to the Headteacher and the Data Protection Officer. Employees should not be bullied into disclosing personal information.

11 Notifying Data Subjects

If we collect Personal Data directly from individuals, we will at the time of collection inform them about the processing including:

- the identity and contact details for the Trust and its Data Protection Officer;
- the purpose or purposes for which we intend to process those Personal Data;
- the types of third parties, if any, with which we will share or to which we will disclose those Personal Data; and
- the means, if any, by which individuals can limit our use and sharing of their Personal Data.

If we receive Personal Data from a source other than the individual we will, except in certain circumstances, provide the individual with the information listed above at the following times:

- within one month of receiving the Personal Data;
- if the Personal Data are to be used for communication with the individual, at the time of the first communication to the individual;
- if a disclosure to another recipient is envisaged by us, at the time of the disclosure to that recipient.

Notifications in the form of Privacy Notices will be in writing or via a link to our website, unless the individual requests an oral notification.

We will also inform individuals whose Personal Data we process that the Trust is the Data Controller with regard to those data and who the Data Protection Officer is.

12 Data security

We will take appropriate security measures against unlawful or unauthorised processing of Personal Data, and against the accidental loss of, or damage to, Personal Data.

We will put in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction. Personal Data will only be transferred to a Data Processor if they agree to comply with those procedures and policies, or if they put in place adequate measures.

Trust staff will be issued with details of their obligations in relation to the security of Personal Data.

All Trust staff must:

- assist the Trust in upholding individuals' data protection rights;
- only act in accordance with the Trust's instructions and authorisation;
- notify the Data Protection Officer immediately of any Personal Data Breaches, allegations of Personal Data Breaches or suspicions of Personal Data Breaches
- comply with the information security standards set out in other Trust policy including the ICT Acceptable use Policy
- comply at all times with the terms of any agreements with the Trust and with their responsibilities under Relevant Data Protection Law;

The Trust will notify the Information Commissioner's Office of any Personal Data Breaches without undue delay.

We will maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

Confidentiality: Only people who are authorised to use the data can access them. Information will not be shared outside the Trust without prior authorisation, or where this is necessary to perform a statutory duty

Integrity: Personal Data should be accurate and suitable for the purpose for which they are processed;

Availability: Authorised users should be able to access the data if they need it for authorised purposes. Personal Data should therefore be stored on the Trust and school's authorised systems instead of on computers, tablets or other media that cannot be accessed by the relevant staff.

Security procedures include:

IT Equipment: Staff must ensure that have read the ICT Acceptable Use Policy before using Trust equipment. Screens should be adjusted so not to show confidential information to passers-by. Staff must log off from their computers, tablets or other devices when left unattended. Only authorised IT equipment should be used to access personal data.

Building Security and Entry controls: All visitors are required to sign in using appropriate systems. Any unauthorised person seen on Trust or school premises should be reported.

Secure lockable storage: Rooms, desks and cupboards and filing cabinets should be kept locked when unattended if they hold any confidential information (personal information is always considered confidential.)

Appropriate sharing and verbal disclosure: When providing personal information verbally, particularly by telephone, it is most important that the individual's identity is verified before any information is disclosed and that conversations occur in a space where information cannot be overheard. Voicemails and messages should not include personal data. Where walky-talky systems are used in school, a protocol for appropriate operation will be made available to staff. Pupil data should not be broadcast over walky-talky channels.

Methods of disposal: Paper documents containing personal information should be shredded when they are no longer needed (in line with the Trust's retention schedule). Digital storage devices should be handed into to relevant staff at the school to be securely destroyed when they are no longer required. A record of disposals should be maintained by each school.

Personal Data on display: All personal data displayed in Trust or school buildings will be limited to what is necessary and pseudonymised where appropriate. If Personal Data is displayed externally, then consent should be sought prior to publication.

Electronic Transport/Transfer of Personal Data: Trust staff will use only approved methods to transport or transfer data as detailed in the ICT Acceptable Use Policy e.g. SharePoint or One Drive. Removable storage devices are not permitted including USB keys, portable hard drives, SD cards or other removable media.

Use of Social Media and Messaging Systems: The Trust recognises the convenience of instant messaging platforms for communication amongst colleagues. The Trust's preferred platform for instant messaging is the Chat function within Microsoft Teams. This provides staff with a simple and secure method of communicating. Use of messaging platforms such as WhatsApp for strictly personal communication between staff members is permitted, provided that all interactions are lawful and maintain professional courtesy, respect, and collegiality.

Photographs and digital images (including video). We use photographs and digital images for a variety of purposes across schools in the Trust, including, but not limited to:

- Capturing development and progress in learning
- School prospectuses and other publications focussed on promoting the schools and the Trust
- Videoconferencing of meetings and other events
- Assemblies and celebration events
- School performances
- Social Media
- Trips and residential outings

Where images of children or staff are used in public areas or made available online via publication on the Trust or schools' websites, parental consent will be checked, or sought, before images are published.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will take reasonable steps to cease using the image as part of our marketing and promotional materials.

Any photographs or videos taken by parents/carers at school events for their own personal use are not covered by data protection law. However, for safeguarding reasons, parents and attendees of publicly accessible school events, should be notified about the appropriate use of such images. This should include notices or announcements explaining that images taken by attendees should not be shared publicly – particularly on social media where accounts are not private.

For other purposes, however, consent to use people's images may not be required.

Use of Online resources: Where the Trust employs the use of mobile apps, cloud-based software or other online resources to aid the delivery of teaching and learning, appropriate checks concerning data protection and ICO Children's Code compliance of suppliers will be undertaken prior to use. The Data Protection Officer should be consulted if the sharing student or staff data is necessary for the use of such resources (this can include the registration and management of user accounts, or the supply of student data to support progress analysis and impact).

Artificial Intelligence: Where technologies planned for use in schools make use of AI and generative AI, these will be risk assessed prior to implementation to ensure data protection compliance. This includes resources and systems used in the delivery of the curriculum and teaching and learning (where pupil data is required) and in support of operational management of the school or Trust (in administration systems). Advice should be sought from the DPO before AI is used for the purposes of profiling or automated decision making. The use of AI technologies to process personal data is prohibited. This includes the recording or transcribing of meetings using AI Bots, the processing of any special categories of personal data for pupils or staff.

Video Conferencing: If videoconferencing technologies are used to support meetings or the delivery of blended/remote learning. The Headteacher should approve this use in the first instance. Staff should first consider any implications for the operation of Trust safeguarding practices when using video conferencing. Guidance is available for all staff on using video conferencing to support teaching and learning.

The Trust shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures designed to implement data-protection principles and to integrate the necessary safeguards into processing activities.

The Trust shall implement appropriate technical and organisational measures for ensuring that, by default, only Personal Data which are necessary for each specific purpose of the processing are processed.

13 Register of processing activities

The Trust must maintain an accurate and up-to-date Information Asset Register of processing activities carried out.

The Trust must record the following information for each processing activity:

- the contact details for the Trust and its Data Protection Officer;
- the purpose or purposes for which the processing activity has occurred;
- descriptions of the categories of individuals involved in the processing activity;
- descriptions of the categories of Personal Data involved in the processing activity;
- descriptions of the categories of recipients of the Personal Data involved in the processing activity;
- details of any transfers to third countries, including documentation of the transfer mechanism safeguards in place;
- retention schedules;
- descriptions of technical and organisational security measures in place relating to the processing activity.

It is the responsibility of all staff to notify the Data Protection Officer of any changes that affect the use of Personal Data, to ensure that the register of processing activities is accurate and kept up to date.

14 Breaches of Personal Data

The Trust must maintain an accurate and up-to-date register of all Personal Data Breaches.
We will take all reasonable steps to minimise the risk of a personal data breach. However, where data breach does occur, it is important that staff are open and honest about it so that it can be managed quickly.

On discovering or causing a breach, or potential breach, the staff member must report it immediately to their Headteacher and the Trust Data Protection Officer using the email address DPO@shineacademies.co.uk

Breaches that occur at a school will normally be investigated by the DPO and Data Protection Lead for that school. However, if this would create a conflict of interest, the investigation will be completed by the DPO and the Trust. Breaches that occur elsewhere within the organisation, or which are caused by a data processor, will also be investigated by the DPO and the Trust.

All breach investigations will:

- assess the likely risk to individuals as a result;
- determine the cause of the issue;
- recommend any actions that might be taken to mitigate that risk; and
- reflect on how to reduce the likelihood that a similar breach will occur in future.

Where an investigation finds risk to rights of individuals is likely, we will report the breach to the ICO. Where feasible, we will do this within 72 hours; otherwise, we will do this without undue delay. Any such reports will be completed by our Data Protection Officer.

In the event that the investigation finds a risk to individuals is high, we will notify those individuals directly and without undue delay.

We will record all personal data breaches, including those that are not reported to the ICO.

15 Protection of Biometric Information of Children

SHINE Academies Trust and its schools do not use any biometrics systems or hold any biometric information about pupils or staff. Should any such systems be introduced, data processing would be in line with all requirements.

Pupils and their parents would be notified before any biometric recognition system was put in place or before their child first took part in it. The school would get written consent before taking any biometric data from their child and first processing it.

Should biometric system(s) be introduced, pupils and their parents would have the right to choose not to use them, and the Trust would provide alternative means of accessing the relevant services for those pupils.

In the above circumstance, where staff members or other adults used the school's biometric system(s), we would also obtain their consent before they first took part in it and would provide alternative means of accessing the relevant service if they objected.

16 Roles and responsibilities

Data Protection Officer

The Data Protection Officer is responsible for supporting the Trust in compliance with Relevant Data Protection Law and with this Policy. The Data Protection Officer reports to the Trust's Chief Executive Officer and Board of Directors but fulfils their data protection functions independently.

The Data Protection Officer for SHINE Academies Trust is provided by Services4 Schools Ltd and can be contacted at DPO@shineacademies.co.uk or by writing to SHINE Academies Trust, Collingwood Road, Bushbury, Wolverhampton, WV10 8DS. Please address letters: **For the attention of the Data Protection Officer.**

Any questions about the operation of this Policy or any concerns that the Policy has not been followed should be referred in the first instance to the Data Protection Officer.

Where a Personal Data Breach has occurred, it will be for the Data Protection Officer to decide whether, under the circumstances and in accordance with Relevant Data Protection Law, the individual concerned must be informed of the breach.

The Data Protection Officer is also responsible for:

- supporting with Data Protection Impact Assessments;
- acting as a contact point for data subjects and the supervisory authority; and
- advising and supporting the schools to meet their data protection obligations
- reporting on their activities, including any advice and recommendations about any data protection issues, directly to the Board of Directors.
- investigating personal data breaches
- responding to information requests

Headteachers (where these are not Data Protection Leads)

Headteachers are responsible for:

- providing day-to-day leadership on data protection issues within their school;
- ensuring their all staff fulfils their duties around data protection; and
- ensuring all their staff complete any training arranged by the school or Trust.

Data Protection Leads

Data Protection Leads are responsible for:

- Liaising with the DPO to advise and supporting the schools to meet their data protection obligations;
- developing and maintaining any procedures and associated documentation required to operationalise this policy;
- ensuring a consistent approach to data protection across the Trust;
- arranging appropriate training and guidance to support staff in meeting their duties under data protection law;
- support in the DPO in investigating breaches of personal data
- support in the DPO in responding to information requests

All Staff

All staff are responsible for:

- processing personal data in accordance with this policy, any associated guidance and any supplementary procedures issued by Headteachers;
- handling records containing personal data in secure manner and in accordance with the Trusts acceptable use of ICT policy;
- treating information in a confidential manner and respecting the privacy and information rights of individuals whose personal data you are given access to;
- recording personal data accurately, in a timely manner using appropriate Trust systems;
- not sharing personal data with individuals, external agencies, suppliers, or other organisations, unless required and appropriate Line Manager approval has been sought in advance;
- informing their Line Manager about any relevant changes to their own personal data, such as a change of address (for example);
- fully participating in all data protection training arranged for them, including familiarising themselves with any updated guidance that is issued by Data Protection Leads
- cooperating with any reasonable request for involvement in compliance monitoring;
- reporting any personal data breach for which they are responsible, as soon as they become aware of it, and
- notifying their Data Protection Lead or DPO if they:
    - have any questions about the operation of this policy or data protection law;
    - have any concerns that this policy is not being followed;
    - are unsure whether they can use personal data in a particular way; or
    - receive a request from an individual to exercise their rights.

17 Using Data Processors

The Trust retains the right to engage by written contract any person or organisation, who is not a member of Trust staff, to process Personal Data on our behalf.

Data Processors must:

- assist the Trust in upholding individuals' data protection rights;
- only act in accordance with the Trust's instructions and authorisation;
- maintain a written record of processing activities carried out on behalf of the Trust and provide this to the Trust within [a reasonable period] following request;
- notify the Trust of Personal Data Breaches without undue delay and maintain a register of breaches
- comply at all times with the terms of any agreements with the Trust and with their responsibilities under Relevant Data Protection Law;

18 Transferring Personal Data to a country outside the UK

Individuals have specific rights with regard to transfers of their Personal Data outside the UK. Circumstances in which the Trust may need to transfer data outside the UK might include use of IT services hosted overseas, arrangement and administration of school trips and cultural exchange projects.

Subject to the requirements applying to Data Processors above, Personal Data we hold may also be processed by staff operating outside the UK who work for us or for one of our suppliers. Those staff may be engaged, among other things, in the processing of payment details and the provision of support services.

We may transfer any Personal Data we hold to a country outside the UK provided that:

- the transfer to the country or countries in question is permitted by Relevant Data Protection Law; and
- any transfer to a country or countries outside the UK is subject the Trust's compliance checks for data processors

Before a transfer of Personal Data is made outside the UK, the following safeguards must be provided to ensure that the rights of Data Subjects and effective legal remedies for Data Subjects are available:

- confirmation by implementing act by the European Commission of the adequacy of the level of protection afforded by the relevant third country;
- standard contractual clauses (SCCs) in accordance with Relevant Data Protection Law must be included in relevant documentation;
- ensuring explicit consent is given by the Data Subject to the proposed transfer after having been informed of the possible risks of such transfer;
- confirmation that the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject;
- confirmation that the transfer is necessary for important reasons of public interest;
- the Data Protection Officer must authorise the transfer.

19 Disclosure and sharing of personal information

We may share Personal Data we hold with staff at any school within the Trust where this is necessary to support teaching and learning, or safeguarding responsibilities.

We may also disclose Personal Data we hold to third parties:

- if we are under a duty to disclose or share an individual's Personal Data in order to comply with any legal obligation;
- in order to enforce or apply any contract with the individual or other agreements; or
- to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of child welfare and fraud protection.

In accordance with the Data Use and Access Act, it is the responsibility of Official Bodies (Police, Courts, Fraud Agencies) to determine and identify the lawful basis for processing in any request for information made to the Trust. Requests which have not identified a lawful basis for processing will be refused.

We may also share Personal Data we hold with selected third parties for the purposes set out in our Privacy Notices

Where an employee of the Trust receives a request to share records containing personal data and this is not already covered by a published Trust Policy or procedure, the permission to share should be approved by an appropriate line manager or the Data Protection Officer, prior to disclosure.

20 Information Requests

Requests for information may take the following forms:

- Requests for education records.
- Freedom of information requests.
- Right of access (Subject access) requests.
- An order from a Court, or a Solicitor to the High Court

Where a person with parental responsibility requests information about a child's educational records, then these should be handled by the appropriate relevant school and advice should be sought from the Data Protection Officer.

If a person makes a request for information under the Freedom of Information Act, then the information should usually be provided unless there are some specific concerns about disclosing the information. Common concerns in the school context may be that information relates to other people, is confidential or legally privileged. If a Freedom of Information request is made and there are any concerns about disclosing information, then the Data Protection Officer should be contacted.

If a person makes a subject access request, then they are requesting the personal information that the Trust has about them. There are exemptions to disclosing some information, but these are more limited as a person has a right to know what information is held on them. If a subject access request is made, then the Data Protection Officer should be contacted immediately.

21 Complaints

If you have a complaint about how your personal data has been handled by SHINE Academies Trust, you should contact the Data Protection Officer in the first instance.

If your complaint does not relate to the processing of personal data, please see the Trust Complaints policy: https://www.shineacademies.co.uk/policies

Complaints or concerns which relate to data protection or information rights should be submitted in writing to DPO@shineacademies.co.uk

The Trust will conduct an internal review into your complaint and respond to you within a calendar month.

If you are unsatisfied with the response the Trust has provided, you have the right to contact the Information Commissioners Office. You can do this online at: https://ico.org.uk/make-a-complaint/data-protection-complaints/

22 Changes to this policy

We reserve the right to change this Policy at any time. This policy will be published on the Trust and school website(s).

Last Review

This Policy was last updated in September 2025