

Privacy Notices

Original Policy Date	September 2026		
Prepared by	Trust & E-Safety Office	Review Frequency	Annual
Approved by	Executive Team		
Version	V1.1	Date of Review	September 2026
Changes	Consolidation of all privacy notices into one policy		
Review Date	Sept 2027 or earlier if there are changes to the relevant legislation		



Version Control

Version	Revision Date	Revised By	Section Revised
V1.1	Sept 2026	L Williams	Consolidated all privacy notices into one policy



Contents Page

1. About The Rose Learning Trust	Page 4
2. Data Protection Principles	Page 4
3. Our Legal Bases for Processing Personal Data	Page 6
4. How We Keep Information Secure	Page 8
5. CCTV	Page 11
6. Your Data Protection Rights	Page 12
7. Contacting Us and Complaints	Page 14
8. Monitoring and Review	Page 15
Section A: Parents and Carers	Page 16
Section B: Children and Pupils	Page 21
Section C: Staff Workforce	Page 24
Section D: Trustees, Governors and Volunteers	Page 29
Section E: Job Applicants	Page 32
Section F: Suppliers, Contractors and Service Providers	Page 35
Section G: Visitors	Page 39



1. About The Rose Learning Trust

The Rose Learning Trust is committed to keeping your personal information safe and secure. This notice is intended to provide information about how the Trust will use of "process" personal data about individuals including:

- Current, past, and prospective pupils
- Parents/carers,
- Staff
- Job applicants
- Trustees and governors
- Volunteers
- Suppliers
- Visitors

This notice provides you with the necessary information regarding your rights and our obligations, and explains how, why, and when we process your personal data.

The Rose Learning Trust's registered office is:

**The Rose Learning Trust
Central Office
Stevens Road Doncaster
DN4 0LT**

We are a company registered in England and Wales under company number **08820308**

We are registered on the Information Commissioner's Office Register; registration number is **ZA 229898**, and act as the Data Controller when processing your data. Our designated Data Protection Officer is Tim Pinto, E-Safety Office and is contactable via email: **tpinto@esafetyoffice.co.uk** or by telephone **01405 494834**.

The trust also has a single point of contact for Data Protection enquiries. Please contact Lyndsey Williams, Rose Learning Trust Governance and Compliance Officer by email at **enquiries@roselearning.co.uk** or by telephone **01302 243528**.

2. Data Protection Principles

The Rose Learning Trust is committed to ensuring that all personal data is processed in accordance with UK data protection legislation. When collecting, using, storing and sharing personal information, the Trust adheres to the following principles:



Lawfulness, Fairness and Transparency

The Trust will only process personal data where there is a lawful basis for doing so. We will be clear about how and why personal information is used and will provide appropriate privacy information to individuals. Personal data will be processed fairly, lawfully and in a transparent manner at all times.

Purpose Limitation

Personal data will be collected for specified, explicit and legitimate purposes and will not be further processed in a way that is incompatible with those purposes. The Trust will only use personal information for the reasons for which it was collected, unless there is a lawful reason to process it for another compatible purpose.

Data Minimisation

The Trust will ensure that personal data collected is adequate, relevant and limited to what is necessary for the purposes for which it is processed. We will only collect and retain information that is required to fulfil our educational, employment, safeguarding, governance, legal and operational responsibilities.

Accuracy

The Trust will take reasonable steps to ensure that personal data is accurate, complete and kept up to date. Individuals are encouraged to inform us of any changes to their personal information so that records can be corrected and maintained accurately. Where inaccuracies are identified, appropriate action will be taken to rectify them without undue delay.

Storage Limitation

Personal data will not be kept for longer than is necessary for the purposes for which it was collected. The Trust manages the retention and disposal of records in accordance with its Records Management Policy, Retention Schedule and statutory requirements. When information is no longer required, it will be securely deleted, anonymised or destroyed.

Security and Confidentiality

The Trust takes the security of personal data seriously and implements appropriate technical and organisational measures to protect information against unauthorised access, loss, misuse, alteration or disclosure. These measures include secure systems, controlled access to information, staff training, confidentiality obligations and the use of data processing agreements with third-party service providers where appropriate.

Accountability

The Trust is responsible for, and able to demonstrate compliance with, these data protection principles. We regularly review our policies, procedures and data protection practices to ensure that personal information is managed appropriately and in accordance with legal requirements.



This commitment applies to all individuals whose personal data is processed by the Trust, including pupils, parents and carers, staff, governors, trustees, volunteers, job applicants, visitors, suppliers and contractors.

3. Our Legal Bases for Processing Personal Data

The Rose Learning Trust processes personal data in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. We will only collect, use, store and share personal information where there is a lawful basis for doing so.

Depending on the purpose of the processing, the Trust may rely on one or more of the following legal bases:

Public Task

The Trust processes personal data where it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in us as an education provider.

This includes activities such as:

- Delivering education and learning programmes.
- Monitoring pupil progress and attainment.
- Providing pastoral support and safeguarding.
- Managing admissions and attendance.
- Supporting pupils with special educational needs and disabilities (SEND).
- Conducting examinations and assessments.
- Managing governance and regulatory responsibilities.

Legal Obligation

The Trust processes personal data where it is necessary to comply with a legal obligation to which we are subject.

This includes, but is not limited to:

- Safeguarding and child protection duties.
- Education legislation and statutory guidance.
- Health and safety requirements.
- Equality and accessibility obligations.
- Employment law requirements.
- Financial audit and accounting requirements.
- Statutory returns to government departments, local authorities and regulators.
- Disclosure of information required by courts, law enforcement agencies or other public bodies with lawful authority.



Legitimate Interests

In certain circumstances, the Trust may process personal data where it is necessary for our legitimate interests or the legitimate interests of a third party, provided those interests do not override the rights and freedoms of the individual concerned.

Examples may include:

- Managing and improving Trust operations.
- Ensuring network and information security.
- Preventing fraud and protecting Trust assets.
- Managing relationships with suppliers, contractors and partners.
- Responding to complaints, claims or legal proceedings.
- Planning, quality assurance, auditing and service improvement activities.

Where legitimate interests are relied upon, the Trust will assess and balance its interests against the rights and freedoms of the individuals whose data is being processed.

Vital Interests

The Trust may process personal data where it is necessary to protect an individual's vital interests or those of another person.

This is most likely to occur in emergency situations where processing is required to protect someone's life, health or welfare, for example:

- Sharing relevant medical information with emergency services.
- Responding to serious safeguarding concerns.
- Protecting a pupil, employee or visitor from immediate harm.

Consent

In certain circumstances, the Trust will seek explicit consent before processing personal data.

Where consent is relied upon, individuals will be informed of:

- What information will be used.
- Why it is being used.
- Who it may be shared with.
- How they can withdraw consent.

Examples may include:

- Use of photographs and videos for promotional purposes.



- Certain educational activities or services provided by third parties.
- Direct marketing communications where consent is required.

Individuals have the right to withdraw their consent at any time. Withdrawal of consent will not affect the lawfulness of processing that took place before consent was withdrawn.

Employment and Social Protection Obligations

For employees, workers, volunteers and job applicants, the Trust may process personal data, including special category data where necessary, to comply with employment law and social protection obligations.

This may include processing information for:

- Recruitment and safer recruitment checks.
- Employment contracts and workforce management.
- Payroll and pension administration.
- Occupational health and wellbeing support.
- Equality monitoring.
- Compliance with safeguarding requirements.
- Managing sickness absence and workplace adjustments.
- Meeting obligations under employment, taxation and social security legislation.

Special Category and Criminal Offence Data

Some of the information processed by the Trust may be classified as special category personal data, such as information relating to health, ethnicity, religion, biometric data or safeguarding matters. The Trust may also process criminal offence data where permitted by law.

Where this type of information is processed, the Trust will ensure that an additional lawful condition under data protection legislation is met and that appropriate safeguards are in place.

Multiple Legal Bases

In many cases, more than one lawful basis may apply to the same processing activity. The Trust will identify and document the most appropriate lawful basis or bases before processing personal data and will keep these under review as part of its accountability obligations.

4. How We Keep Information Secure

The Rose Learning Trust recognises the importance of protecting personal data and is committed to ensuring that appropriate technical and organisational measures are in place to safeguard information against unauthorised access, accidental loss, misuse, disclosure, alteration or destruction. We take our responsibility for information security seriously and continually review our arrangements to ensure personal data remains protected.



Security Measures

The Trust maintains a range of physical, technical and organisational security measures designed to protect personal information, including:

- Secure storage of paper and electronic records.
- Encryption and password protection where appropriate.
- Secure backup and recovery procedures.
- Anti-virus, anti-malware and network security controls.
- Regular security updates and patch management.
- Staff training and awareness on data protection and information security.
- Procedures for responding to and managing data breaches.

All staff, governors, trustees, volunteers and contractors who access personal data are expected to maintain confidentiality and comply with the Trust's data protection and information security requirements.

ICT Systems

The Trust uses a range of approved ICT systems and cloud-based services to support education, administration, communication, governance and business operations. These systems are selected to ensure appropriate levels of security and compliance with data protection legislation.

Where personal data is processed through third-party systems, the Trust takes reasonable steps to ensure appropriate security measures and contractual safeguards are in place.

Access Controls

Access to personal data is restricted to those individuals who require it to perform their role. The Trust applies appropriate access controls to ensure information is only available to authorised users.

These controls may include:

- User account authentication.
- Password and multi-factor authentication requirements.
- Role-based permissions.
- Restricted administrator access.
- Monitoring and auditing of system access and activity.

Access rights are reviewed regularly and removed promptly when no longer required.

Data Sharing Agreements

Where personal data is shared with external organisations, service providers or partner agencies, the Trust will ensure that appropriate data sharing agreements, contracts or data processing agreements are in place where required.



These agreements set out:

- The purpose of the data sharing.
- The responsibilities of each organisation.
- Security expectations and requirements.
- Data retention and disposal arrangements.
- Requirements relating to confidentiality and lawful processing.

The Trust only shares information where there is a lawful basis to do so and where appropriate safeguards are in place.

International Transfers

Some providers used by the Trust may process information outside the UK. Where this occurs, appropriate safeguards will be in place in accordance with UK GDPR requirements.

Supplier Due Diligence and Assurance

Before engaging third-party suppliers who may process personal data on behalf of the Trust, appropriate due diligence checks are carried out. These checks help ensure suppliers can demonstrate compliance with relevant data protection and information security requirements.

The Trust may consider factors such as:

- Security certifications and standards.
- Privacy and security policies.
- Data hosting arrangements.
- Incident management procedures.
- Data processing and international transfer arrangements.
- Compliance with UK data protection legislation.

Supplier arrangements are reviewed periodically throughout the contract lifecycle.

Retention Schedules

The Trust retains personal information only for as long as necessary to fulfil the purpose for which it was collected and to meet legal, regulatory, safeguarding, financial and operational requirements.

Personal information is retained in accordance with the Trust's Records Management Policy and Retention Schedule which is based on statutory, regulatory and operational requirements.

Retention periods are determined with reference to:

- Statutory and regulatory requirements.



- Department for Education guidance.
- Employment and taxation legislation.
- Limitation periods for legal claims.
- Business and operational needs.

At the end of the applicable retention period, information will be securely deleted, anonymised or destroyed.

Records Management Policy

The Trust operates a Records Management Policy which defines how information is created, stored, retained, archived and disposed of throughout its lifecycle.

The policy helps ensure that:

- Records are maintained accurately and consistently.
- Information can be accessed when required.
- Retention periods are applied appropriately.
- Records are disposed of securely and confidentially.
- The Trust complies with legal and regulatory obligations.

Further information regarding the Trust's records management and retention arrangements can be obtained by contacting the Trust's Data Protection Officer or the Governance and Compliance Officer.

Monitoring and Review

The Trust regularly reviews its security arrangements, policies and procedures to ensure they remain effective and appropriate. Security measures may be updated from time to time in response to changes in technology, legislation, emerging threats or organisational

5. CCTV

To help maintain a safe and secure environment for pupils, staff, visitors and other members of the school community, The Rose Learning Trust operates Closed-Circuit Television (CCTV) systems at Trust sites where appropriate. CCTV is used to support safeguarding, security, crime prevention and detection, the protection of Trust property, and the health and safety of individuals on our premises.

The Trust processes CCTV images in accordance with UK data protection legislation and relevant guidance issued by the Information Commissioner's Office (ICO). CCTV recordings are only accessed by authorised personnel where there is a legitimate business, safeguarding, security or legal reason to do so.

Where CCTV is in operation, appropriate signage will be displayed to make individuals aware that recording is taking place. CCTV footage will be retained only for as long as necessary and will be securely managed in accordance with the Trust's information security and records management arrangements.



Further information about how CCTV is used, managed, accessed, retained and disclosed, including the rights of individuals in relation to CCTV recordings, can be found in the Trust's CCTV Policy, which is available on the Trust website or upon request from the Trust's Data Protection Officer or Governance and Compliance Officer.

6. Your Data Protection Rights

Under UK data protection legislation, individuals have a number of important rights regarding how their personal information is collected, used, stored and shared. These rights are not absolute and may be subject to certain exemptions or restrictions depending on the circumstances. The Rose Learning Trust will consider all requests fairly and in accordance with applicable legislation.

Right of Access

You have the right to request access to the personal information the Trust holds about you and, where applicable, your child. This is commonly known as a Subject Access Request (SAR).

When responding to a request, we will:

- Confirm whether we process your personal data.
- Provide a description of the personal information held.
- Explain why it is being processed.
- Explain how long it will be retained.
- Identify the source of the information where it was not obtained directly from you.
- Explain who the information has been or may be shared with.
- Provide a copy of the information where appropriate.

Right to Rectification

You have the right to request that inaccurate, incomplete or out-of-date personal information is corrected. The Trust encourages individuals to notify us promptly of any changes to their personal information to help ensure records remain accurate.

Right to Erasure

In certain circumstances, you have the right to request the deletion or removal of your personal data where there is no lawful reason for the Trust to continue processing it.

This right does not apply where the Trust is legally required to retain information or where another lawful basis for processing exists.

Right to Restrict Processing

You have the right to request that the Trust limits the way in which your personal data is used. This may apply where:



- You believe information is inaccurate.
- The processing is unlawful, but you do not want the information deleted.
- The Trust no longer requires the information, but you need it for legal purposes.
- You have objected to processing and a decision is pending.

Right to Object

You have the right to object to the processing of your personal data in certain circumstances, including:

- Processing based on the Trust's legitimate interests.
- Direct marketing communications.
- Processing for research or statistical purposes where applicable.

The Trust will consider all objections and determine whether there are compelling lawful grounds to continue processing the information.

Right to Data Portability

Where processing is based on consent or contract and carried out by automated means, you may have the right to receive your personal information in a structured, commonly used and machine-readable format and, where technically feasible, request that it is transferred directly to another organisation.

Rights Relating to Automated Decision-Making

You have the right not to be subject to a decision based solely on automated processing, including profiling, where that decision produces legal effects or similarly significant effects on you, except where permitted by law.

The Trust does not routinely make significant decisions solely by automated means. Where automated processing is used, appropriate safeguards will be in place.

Right to Withdraw Consent

Where the Trust relies on your consent to process personal data, you have the right to withdraw that consent at any time. Withdrawal of consent will not affect the lawfulness of any processing carried out before consent was withdrawn.

Exercising Your Rights

To exercise any of the rights outlined in this Privacy Notice, please contact your school in the first instance, or alternatively contact the Trust's Data Protection Officer or Governance and Compliance Officer using the contact details provided in this notice. Requests will be managed in accordance with applicable data protection legislation and statutory timescales.



Right to Complain

If you are unhappy with how the Trust has processed your personal information, you have the right to raise a concern through the Trust's Data Protection Complaints Procedure and to lodge a complaint with the Information Commissioner's Office (ICO).

7. Contacting Us and Complaints

The Rose Learning Trust is committed to protecting personal information and handling data protection concerns fairly, transparently and in accordance with UK data protection legislation. If you have any questions about this Privacy Notice, wish to exercise your data protection rights, or have concerns about how your personal information has been processed, please contact us using the details below.

Data Protection Officer (DPO)

The Trust has appointed an independent Data Protection Officer (DPO) who provides advice and oversight regarding compliance with data protection legislation.

Tim Pinto - E-Safety Office
Email: tpinto@esafetyoffice.co.uk
Telephone: 01405 494834

Trust Data Protection Single Point of Contact

The Trust has a designated single point of contact for data protection matters, including requests relating to personal data, privacy concerns and data protection enquiries.

Lyndsey Williams - Governance and Compliance Officer
The Rose Learning Trust
Email: enquiries@roselearning.co.uk
Telephone: 01302 243528

Data Protection Complaints

The Trust takes all concerns regarding the use of personal information seriously and aims to resolve complaints promptly and effectively.

If you have a concern about how your personal data has been collected, used, shared, retained or otherwise processed, you should raise your concern in accordance with the Trust's Data Protection Policy and Data Protection Complaints Procedure.

Complaints will be investigated in a timely manner and handled in line with the Trust's published procedures. Individuals will not be disadvantaged for raising a genuine concern about the handling of their personal information.



Where appropriate, we encourage individuals to contact the Trust in the first instance so that we have an opportunity to understand and resolve the issue. If you remain dissatisfied following the Trust's response, or you believe that your personal information has been processed unlawfully, you have the right to make a complaint to the Information Commissioner's Office (ICO), the UK's independent regulator for data protection matters.

Information Commissioner's Office (ICO)

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

Telephone: 0303 123 1113

Address:

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF

Further Information

Further information about how the Trust processes and protects personal data can be found in the following Trust documents:

- Data Protection Policy
- Data Protection Complaints Procedure
- Records Management Policy
- CCTV Policy
- Freedom of Information Publication Scheme
- Information Security and Acceptable Use Policies

Copies of these documents are available on the Trust website or upon request.

8. Monitoring and Review

This Privacy Notice will be reviewed annually and may be updated to reflect changes in legislation, guidance or Trust practices. The latest version will always be available on the Trust website.



Section A: Parents and Carers

Who This Section Applies To

This section applies to:

- Parents, carers and guardians of current pupils.
- Parents and carers of prospective pupils.
- Parents and carers of former pupils where the Trust continues to retain information in accordance with its retention schedule.

Why We Process Personal Data About Parents, Carers and Pupils

The Trust processes personal data in order to fulfil its duties and responsibilities as an education provider and to support the education, wellbeing, safeguarding and development of pupils. We also process information to meet our statutory obligations and to manage the day-to-day operation of our schools.

We may obtain information directly from parents and carers, from previous schools, local authorities, health professionals, educational professionals and government departments where this is necessary and lawful.

Information We Collect

The personal information we may collect, use, store and share includes:

Parent and Carer Information

- Names and contact details.
- Postal addresses.
- Emergency contact information.
- Communication preferences.
- Information relating to payments for services such as school meals, trips and educational activities.

Pupil Information

- Personal identifiers, including name, date of birth and unique pupil number.
- Attendance information, including sessions attended, absence data and reasons for absence.
- Assessment and attainment information.
- Pupil and curriculum records.
- Ethnicity and free school meal eligibility information.
- Special Educational Needs and Disabilities (SEND) information.
- Education, Health and Care Plan (EHCP) information.
- Medical information, including physical and mental health information where required.
- Behaviour records, including exclusions and alternative provision arrangements.
- Safeguarding information, including court orders and professional involvement.



- Child in Need and Child Protection information.
- Details of support plans, care packages and support providers.
- School trip information and consent records.
- Information required to provide school meals.
- Information relating to educational software and learning platforms.
- Information required to meet statutory returns, auditing and funding requirements.

This list is not exhaustive and may be updated where necessary to fulfil the Trust's educational, legal and safeguarding responsibilities.

How We Use This Information

We use parent, carer and pupil information to:

- Provide education and learning opportunities.
- Deliver extracurricular activities.
- Safeguard and promote the welfare of pupils.
- Provide pastoral, welfare and medical support where appropriate.
- Monitor educational progress and attainment.
- Identify and provide additional support.
- Allocate teaching and support resources effectively.
- Enable participation in national assessments and examinations.
- Maintain accurate pupil records.
- Communicate effectively with parents and carers.
- Support management planning, forecasting, research and statistical analysis.
- Monitor use of Trust IT systems in accordance with Trust policies.
- Confirm the identity of prospective pupils and parents/carers.
- Administer school meals, trips and educational visits.
- Create invoices and process payments.
- Obtain professional advice and insurance where required.
- Fulfil legal and regulatory obligations, including safeguarding and health and safety responsibilities.
- Keep parents and carers informed about school activities, events, newsletters, emergency arrangements and closures.

Photographs, Video and Promotional Materials

The Trust may use photographs or video images of pupils for legitimate educational purposes, including learning journals, displays and classroom activities.

Photographs or videos intended for promotional purposes, including websites, social media, newsletters or marketing materials, will only be used where the appropriate consent has been obtained.

The Trust may engage professional school photographers whose photographs are stored within approved Trust systems. Parents and carers may be offered the opportunity to purchase photographs, but there is no obligation to do so. Appropriate data-sharing arrangements are in place with such providers.



Marketing Communications

Where consent has been provided, the Trust may send information by email or text message about:

- School events.
- Fundraising activities.
- Charitable initiatives.
- Community activities.
- Relevant services for children and families.

Consent may be withdrawn at any time by contacting the school office. The Trust does not sell personal data.

How We Collect Information

Information is obtained:

- Directly from parents and carers.
- Through admission and enrolment processes.
- Through routine updates provided by families.
- From previous schools via the Common Transfer File (CTF) process.
- From local authorities, health services and other professionals where appropriate and lawful.

Parents and carers are encouraged to ensure that contact and personal information remains accurate and up to date.

How Long We Keep Information

The Trust retains parent and pupil information while a pupil attends one of our schools and, where necessary, after they leave in accordance with legal, regulatory and operational requirements. Information is retained in line with the Trust Records Management Policy and retention schedule.

Who We Share Information With

Where lawful and necessary, we may share information with:

- Local authorities.
- The Department for Education (DfE).
- Family members and authorised representatives.
- Other schools within The Rose Learning Trust.
- Schools attended after a pupil leaves the Trust.
- Examination and awarding bodies.
- Ofsted.
- Auditors.
- Financial organisations.
- Health professionals and health authorities.



- Social care and welfare organisations.
- Professional advisers and consultants.
- Charities and voluntary organisations supporting pupil needs.
- Police, courts and tribunals.
- ICT support providers.
- Educational software providers.
- School meal providers where allergy information is required.
- Other suppliers and service providers engaged by the Trust.

Examples of systems and providers used by the Trust include:

- Arbor.
- CPOMS.
- ParentPay.
- ParentMail.
- Free School Meal Eligibility services.
- Educational software platforms.
- Assessment systems.
- Microsoft Outlook and Microsoft 365 services.
- Cool Milk.

This list is not exhaustive and may change as services develop.

Sharing Information with Third Parties Based on Consent

Where appropriate, and where consent has been provided, information may also be shared with:

- Peripatetic music teachers.
- Providers of extracurricular activities.
- After-school club providers.
- Other approved organisations supporting educational opportunities for pupils.

National Pupil Database

The Trust is required by law to provide information about pupils to the Department for Education through statutory returns including the school census and early years census. Some of this information is stored within the National Pupil Database (NPD).

The NPD supports:

- Educational research and analysis.
- Production of statistics.
- Development of education policy.

Provision of information, advice and guidance designed to promote the education and wellbeing of children.



The Department for Education applies strict controls governing who may access this information and how it may be used. Organisations granted access must comply with robust security, confidentiality and data-handling requirements.



Section B: Children and Pupils

Who This Section Applies To

This section applies to all children and pupils attending schools within The Rose Learning Trust. It explains, in a way that is easier to understand, how we use information about you.

What Is Personal Data?

Personal data is information that can identify you. This includes things such as:

- Your name.
- Your date of birth.
- Your photograph.
- Your address.
- Your email address.
- Information about your learning and progress at school.

Some information is more sensitive and needs extra protection. This may include information about your health, wellbeing, support needs or safeguarding concerns.

What Information Do We Collect?

To help us provide you with an education and keep you safe, we may collect information such as:

- Your name and contact details.
- Information about your parents or carers.
- Attendance information.
- Assessment and attainment information.
- Behaviour and achievement records.
- Medical information.
- Information about allergies or dietary requirements.
- Information about any additional support you may need.
- Safeguarding and welfare information where necessary.

Why Do We Need Your Information?

We use your information so that we can:

- Know who you are.
- Teach and support you.
- Keep you safe and healthy.
- Help you learn and make progress.
- Provide support if you need extra help.
- Contact your parents or carers when necessary.
- Meet the legal responsibilities schools have.



Everyone is different, so we may need to know things such as what to do if you become unwell, whether there are certain foods you cannot eat, or whether there is extra support we can provide to help you with your learning.

Who Can See Your Information?

Your information is important and we only share it with people who need to know.

This may include:

- Your teachers.
- School leaders.
- Support staff.
- School nurses and healthcare professionals.
- Other professionals who help support your education, wellbeing or safety.
- Government organisations where we are required by law to share information.

We only share information when there is a valid reason to do so and where appropriate safeguards are in place.

How Long Do We Keep Your Information?

We keep your information while you attend one of our schools. When you move to another school, we will normally transfer relevant information to help support your education.

Some records may be kept after you leave school in accordance with legal and statutory requirements. In many cases, pupil records are retained by the last school attended until you reach the age of 25.

Your Rights

You have rights over your information, including the right to know:

- What information we hold about you.
- Why we use it.
- Who we share it with.
- How we keep it safe.

As you get older, you gain additional rights over how your information is used. From the age of 13, you may be able to make certain requests about your personal information yourself, depending on the circumstances.

More information about your rights can be found in the Your Data Protection Rights section of this Privacy Notice.

Who Makes the Rules?

The Trust must follow data protection laws set by the government. These laws help make sure that personal information is used fairly and kept safe.

The Information Commissioner's Office (ICO) is the UK's independent authority for data protection and makes sure organisations use people's information properly.



Further Information

If you have questions about your information or this Privacy Notice, you can:

- Speak to your teacher.
- Speak to a trusted adult in school.
- Ask your parent or carer to help you understand this notice.
- Refer to the Trust website for more information about data protection and privacy.

The Trust is committed to keeping your information safe and making sure you understand how and why it is used.



Section C: Staff Workforce

Who This Section Applies To

This section applies to current and former employees, workers, agency staff, contractors engaged in a personal capacity, apprentices, trainees and volunteers working within The Rose Learning Trust. It explains how the Trust collects, uses, stores and shares workforce information for employment and workforce management purposes.

Information We Collect

The Trust may collect, use, store and share a range of workforce information, including:

Personal Information

- Name and contact details.
- Employee, teacher or payroll reference numbers.
- National Insurance number.
- Date of birth.
- Emergency contact and next of kin details.

Employment Information

- Job title and role.
- Contract details.
- Start date and employment history.
- Working hours and salary details.
- Qualifications and professional memberships.
- Training and development records.
- Performance and appraisal information.
- Disciplinary, grievance and employment relations records.

Recruitment Information

- Application forms and CVs.
- References.
- Right to work documentation.
- Identity verification documents.
- Disclosure and Barring Service (DBS) information where required.
- Interview and assessment records.

Payroll and Financial Information

- Bank account details.



- Payroll records.
- Tax status information.
- Pension information.
- Expenses and reimbursement records.

Attendance and Wellbeing Information

- Absence records.
- Sickness and occupational health information.
- Relevant medical information where necessary.
- Workplace adjustment information.

ICT and Security Information

- Information relating to the use of Trust ICT systems.
- User account and network activity data.
- Photographs used for identification badges and internal systems.
- Security and access records.

Special Category Data

Where necessary and lawful, the Trust may process special category personal data, including information relating to:

- Race and ethnicity.
- Religious or philosophical beliefs.
- Trade union membership.
- Health and medical conditions.
- Sickness and absence records.
- Equality monitoring information.

This list is not exhaustive and may change where necessary to fulfil the Trust's legal, employment and operational responsibilities.

How We Collect Information

The Trust collects workforce information in a variety of ways, including:

- Recruitment and application processes.
- Employment contracts and starter documentation.
- Information provided directly by employees.
- HR and payroll systems.
- Performance management and appraisal processes.
- Meetings, interviews and assessments.
- Sign-in and sign-out systems.



- CCTV and security systems.
- References from previous employers.
- DBS checks and safeguarding checks where permitted by law.
- Professional bodies and qualification providers.

Some information is mandatory in order for the Trust to meet legal, contractual and safeguarding obligations. Where information is optional, individuals will be informed at the point of collection.

Why We Use Workforce Information

The Trust processes workforce information to:

- Administer contracts of employment.
- Enable the payment of salaries and expenses.
- Manage pensions and employee benefits.
- Facilitate safer recruitment processes.
- Meet safeguarding obligations.
- Support workforce planning and resource management.
- Manage attendance, leave and absence.
- Support performance management and professional development.
- Monitor equality, diversity and inclusion.
- Comply with employment, education and safeguarding legislation.
- Meet audit, financial and regulatory requirements.
- Support business continuity and operational management.
- Maintain the security of Trust premises, systems and information.
- Produce statutory workforce returns and reporting requirements.

Who We Share Workforce Information With

The Trust will only share workforce information where there is a lawful basis to do so.

Information may be shared with:

- HM Revenue and Customs (HMRC).
- Pension providers and pension schemes.
- The Disclosure and Barring Service (DBS).
- Local Authorities.
- Healthcare, social care and welfare professionals.
- Schools within The Rose Learning Trust.
- Regulatory bodies, including Ofsted.
- Professional advisers and consultants.
- Auditors.
- Service providers supporting payroll, HR, banking and employee wellbeing.
- Law enforcement agencies.
- Courts and tribunals.



- Trade unions and professional associations.
- Government departments.
- Research and survey organisations where appropriate.

Where consent has been provided, information may also be shared with:

- Mortgage providers.
- Housing associations.
- Landlords.
- Credit reference agencies.

In the event of a TUPE transfer, the minimum necessary personal information will be shared with the prospective employer in accordance with legal requirements.

Department for Education Workforce Data

The Trust is required by law to submit workforce information to the Department for Education (DfE) through statutory workforce census returns.

This information helps the DfE to:

- Monitor the school workforce.
- Inform education policy.
- Support workforce planning.
- Analyse workforce diversity and effectiveness.
- Support educational research and statistical reporting.

The DfE maintains strict controls regarding access, security, retention and use of workforce data and may share information with approved organisations for research, analysis and policy purposes where permitted by law.

Photographs and Staff Information

The Trust may use staff photographs for:

- Identification badges.
- Internal systems and directories.
- Security purposes.
- School websites and publications where appropriate.

Staff names, roles and work contact details may also be displayed on school websites and notice boards in accordance with Department for Education guidance and the legitimate interests of the Trust in supporting communication with pupils, parents and the wider school community.



ICT Monitoring

To protect Trust systems, users and information assets, the Trust may monitor the use of its ICT systems and networks in accordance with Trust policies and applicable legislation. This may include monitoring email, internet usage, user accounts and access logs where necessary for security, safeguarding, operational or legal purposes.

Storage and Retention

Workforce information is stored securely within personnel files, HR and payroll systems, Trust ICT systems and other authorised record management systems. Access is restricted to authorised personnel who require the information to perform their duties.

The Trust retains workforce information in accordance with its Records Management Policy and Retention Schedule. Information will be securely deleted, archived or destroyed when it is no longer required.

Further Information

Further information regarding the Trust's processing of workforce information can be found in:

- The Trust Data Protection Policy.
- Staff ICT Acceptable Use Policies.
- Records Management Policy.
- Safer Recruitment Procedures.
- CCTV Policy.
- Employee Handbook and related HR policies.

These documents are available through the Trust or individual schools upon request.



Section D: Trustees, Governors and Volunteers

Who This Section Applies To

This section applies to individuals working with The Rose Learning Trust in a voluntary governance or support capacity, including:

- Trustees.
- Members of Local Governing Bodies.
- Academy Councillors and Committee Members (where applicable).
- Volunteers supporting Trust or school activities.

Information We Collect

The Trust may collect, use, store and share personal information relating to trustees, governors and volunteers, including:

- Names and contact details.
- References.
- Evidence of qualifications.
- Employment details and work history where relevant.
- Information relating to business, financial and pecuniary interests.
- Disclosure and Barring Service (DBS) information and outcomes.
- Emergency contact and next of kin details.

Special Category Personal Data

Where necessary and permitted by law, the Trust may also process special category personal data, including information relating to:

- Race and ethnicity.
- Religious or philosophical beliefs.
- Political opinions.
- Sexual orientation.
- Disabilities.
- Access requirements and reasonable adjustments.

This list is not exhaustive and may be supplemented where necessary to meet legal, safeguarding, governance or operational requirements.

Why We Use This Information

The Trust processes governance and volunteer information to:



- Establish and maintain effective governance arrangements.
- Support the operation and oversight of the Trust and its schools.
- Meet statutory and regulatory obligations relating to governance.
- Publish and share governance information where required by law.
- Facilitate safer recruitment and safeguarding processes.
- Undertake equality, diversity and inclusion monitoring.
- Manage volunteer arrangements.
- Ensure appropriate access arrangements and reasonable adjustments can be provided where required.
- Protect the safety and security of pupils, staff, volunteers and Trust premises.

How We Collect Information

Information is collected directly from trustees, governors and volunteers through:

- Appointment and recruitment processes.
- Application and declaration forms.
- Governance registration and compliance checks.
- DBS and safeguarding checks.
- Training and induction processes.
- Ongoing communications and governance activities.

While much of the information collected is required to enable the Trust to fulfil its legal and safeguarding responsibilities, some information may be provided on a voluntary basis. Individuals will be informed when information is mandatory and of any consequences of not providing it.

Who We Share Information With

The Trust does not share information unless there is a lawful basis for doing so.

Where required by law, or where necessary for governance, safeguarding or operational purposes, information may be shared with:

- Government departments and agencies.
- The Department for Education (DfE).
- The Local Authority.
- Governance support providers.
- Professional advisers and consultants.
- Employment and recruitment agencies.
- Service providers acting on behalf of the Trust.
- Police, courts and other law enforcement agencies.

Information relating to trustees and governors may be published or disclosed where required by legislation, regulatory guidance or governance transparency requirements.



Governance Transparency and Statutory Requirements

As an academy trust, The Rose Learning Trust is required to publish and share certain information relating to its governance arrangements. This may include information about trustees, governors, governance roles, attendance, terms of office and declarations of interests where required by legislation or regulatory guidance.

The Trust will only publish information that it is legally required or permitted to disclose and will ensure that personal information is handled appropriately and proportionately.

International Transfers

Where personal data is transferred outside the United Kingdom or European Economic Area through approved systems or service providers, the Trust will ensure appropriate safeguards are in place in accordance with data protection legislation.

Storage and Retention

The Trust maintains secure records relating to trustees, governors and volunteers. Information is stored securely and access is restricted to authorised individuals who require the information to perform their duties.

Personal information is retained and disposed of in accordance with the Trust's Records Management Policy and Retention Schedule. When an individual's relationship with the Trust ends, records will be retained only for as long as necessary and then securely destroyed or deleted.

Safeguarding and Vetting

As part of the Trust's commitment to safeguarding and promoting the welfare of children and young people, governance volunteers may be subject to appropriate pre-appointment and ongoing vetting checks, including DBS checks and eligibility verification where required by legislation and statutory guidance.

Further Information

Further information regarding the processing of personal data relating to trustees, governors and volunteers can be found in:

- Data Protection Policy.
- Governance Handbook and Scheme of Delegation.
- Records Management Policy.
- Safeguarding and Child Protection Policy.
- DBS and Safer Recruitment Procedures.
- Register of Interests Policy.
- CCTV Policy.

These documents are available on the Trust website or upon request from the Trust



Section E: Job Applicants

Who This Section Applies To

This section applies to individuals applying for employment opportunities within The Rose Learning Trust. It explains how the Trust collects, uses, stores and shares personal information during the recruitment and selection process.

Information We Collect

The Trust may collect, use, store and share personal information relating to job applicants, including:

- Names and contact details.
- Application forms, CVs and covering letters.
- Copies of right to work documentation.
- References from current and previous employers.
- Evidence of qualifications and professional certifications.
- Employment history and work experience.
- Training records and professional memberships.
- Interview notes and recruitment assessment records.

Special Category Personal Data

Where necessary and lawful, the Trust may also process special category personal data, including information relating to:

- Race and ethnicity.
- Religious or philosophical beliefs.
- Sexual orientation.
- Political opinions.
- Disability information and access requirements.

Criminal Offence Data

As part of the Trust's safeguarding responsibilities, we may collect and process information relating to criminal convictions, cautions or Disclosure and Barring Service (DBS) checks where permitted by law and relevant to the role being applied for.

The Trust may also receive information from other organisations, including schools, local authorities, social services and the Disclosure and Barring Service, where appropriate and lawful.

Why We Use This Information

We process applicant information to support the recruitment process, including to:



- Assess experience, qualifications and suitability for a role.
- Facilitate safer recruitment and safeguarding checks.
- Verify identity, qualifications and right to work in the United Kingdom.
- Enable equality monitoring and reporting.
- Make reasonable adjustments and provide appropriate access arrangements during recruitment.
- Communicate with applicants throughout the recruitment process.
- Fulfil legal and regulatory obligations.

Recruitment Communications

Where consent has been provided, the Trust may send information regarding future vacancies, recruitment campaigns or employment opportunities. Consent can be withdrawn at any time.

The Trust does not currently use automated decision-making or profiling as part of its recruitment processes. Should this change, applicants will be informed and provided with details of their rights.

How We Collect Information

Most of the information processed during recruitment is provided directly by applicants through:

- Application forms.
- CVs and supporting statements.
- Interviews and assessment activities.
- Recruitment documentation and correspondence.

We may also obtain information from:

- Referees.
- Previous employers.
- Local authorities.
- Government departments and agencies.
- Police forces, courts and tribunals where relevant and lawful.

Some information is mandatory to enable the Trust to comply with legal, safeguarding and employment obligations. Applicants will be informed where information is required and of any consequences of failing to provide it.

Who We Share Information With

The Trust will only share applicant information where there is a lawful basis for doing so.

Where necessary, information may be shared with:

- Local authorities for safeguarding purposes.
- Professional advisers and consultants supporting recruitment activities.



- Employment and recruitment agencies.
- Disclosure and Barring Service (DBS).
- Other organisations where required by law or regulatory requirements.

Where personal data is transferred outside the United Kingdom, appropriate safeguards will be implemented in accordance with data protection legislation.

Storage and Retention

Personal information collected as part of the recruitment process is stored securely in accordance with the Trust's Records Management Policy. Appropriate technical and organisational security measures are in place to prevent information from being lost, altered, accessed or disclosed without authorisation.

Successful applicants' information will be transferred to their personnel file and processed in accordance with the Staff Workforce section of this Privacy Notice.

Information relating to unsuccessful applicants will be retained only for as long as necessary in accordance with the Trust's retention schedule and then securely deleted or destroyed.

Safer Recruitment

The Trust is committed to safeguarding and promoting the welfare of children and young people. As part of our safer recruitment procedures, applicants may be subject to:

- Identity verification.
- Right to work checks.
- Qualification verification.
- Employment history checks.
- Reference checks.
- Disclosure and Barring Service (DBS) checks where required.

These checks help ensure the Trust meets its safeguarding obligations towards pupils and complies with statutory guidance.

Further Information

Further information regarding the processing of applicant information can be found in:

- Data Protection Policy.
- Safer Recruitment Policy.
- Records Management Policy.
- Recruitment and Selection Procedures.
- Safeguarding and Child Protection Policy.

These documents are available on the Trust website or upon request.



Section F: Suppliers, Contractors and Service Providers

Who This Section Applies To

This section applies to suppliers, contractors, consultants, service providers and other organisations that provide goods or services to The Rose Learning Trust, including their employees, representatives, agents and subcontractors where personal data is processed in connection with a contractual relationship.

Information We Collect

The Trust may collect, use, store and share personal information relating to suppliers and their representatives, including:

- Names and contact details of supplier representatives, employees and agents.
- Job titles and business contact information.
- References, CVs and employment history where collected as part of a procurement, tendering or engagement process.
- Bank account details and financial information where relevant, particularly for sole traders and individual contractors.
- Information required to establish, manage and fulfil contractual arrangements.
- Information relating to business, financial or pecuniary interests.
- Visitor records, including company details, arrival and departure times and vehicle registration details when attending Trust premises.

Special Category Personal Data

In limited circumstances, the Trust may process special category personal data where necessary and lawful, including:

- Information relating to accessibility requirements or reasonable adjustments.
- Photographs used for identification purposes.
- CCTV images recorded while visiting Trust premises.

The Trust may also receive information about suppliers and their representatives from other organisations, including schools, local authorities and public bodies where appropriate and lawful.

Why We Use This Information

The Trust uses supplier information to:

- Assess potential suppliers and contractors.
- Conduct procurement, tendering and due diligence activities.
- Establish and manage contractual relationships.
- Process invoices and make payments.



- Maintain accurate supplier records.
- Verify the identity of individuals attending Trust premises.
- Maintain safeguarding, health and safety and site security arrangements.
- Record and manage visits to schools and Trust premises.
- Meet legal, regulatory and audit requirements.

The Trust does not currently use automated decision-making or profiling in relation to supplier information.

How We Collect Information

Most supplier information is collected directly from suppliers, contractors or their representatives during:

- Procurement and tendering exercises.
- Supplier onboarding processes.
- Contract negotiations and management activities.
- Site visits and access arrangements.

The Trust may also receive information from:

- Local authorities.
- Government departments and agencies.
- Police forces, courts and tribunals.
- Professional references and due diligence sources.

Where information is mandatory, suppliers will be informed of the requirement and any implications of not providing the requested information.

Who We Share Information With

The Trust will only share supplier information where there is a lawful basis to do so.

Information may be shared with:

- Local authorities.
- Government departments and agencies.
- Ofsted and other regulatory bodies.
- Auditors and external assurance providers.
- Professional advisers and consultants.
- Health authorities and health and social care organisations where appropriate.
- Security organisations.
- Police, courts and tribunals.
- Professional bodies.
- Other service providers where necessary to support contractual arrangements.
- The organisation or company that an individual supplier representative represents.



Where legally required or necessary to protect children, staff or Trust interests, information may also be shared for safeguarding, legal, regulatory or investigative purposes.

Procurement and Due Diligence

The Trust may process supplier information as part of procurement, contract management and supplier assurance processes. This may include:

- Verification of supplier credentials.
- Financial and compliance checks.
- Assessment of suitability to provide services.
- Evaluation of safeguarding, security and regulatory compliance where relevant to the services being provided.

These checks help ensure that the Trust meets its legal, financial and safeguarding responsibilities.

Visitors to Trust Premises

Where supplier representatives visit Trust premises, additional information may be collected to support:

- Site security.
- Safeguarding arrangements.
- Health and safety requirements.
- Emergency evacuation procedures.

The Trust's Visitor Privacy Notice may also apply in these circumstances.

Storage and Retention

Supplier information is stored securely and retained in accordance with the Trust's Records Management Policy and Retention Schedule. Information relevant to contracts and financial transactions may be retained for statutory, audit and regulatory purposes.

When information is no longer required, it will be securely deleted, anonymised or disposed of in accordance with Trust procedures.

International Transfers

Where personal data is transferred outside the United Kingdom, the Trust will ensure that appropriate safeguards are in place and that any transfer complies with UK data protection legislation. Suppliers may request further information regarding any applicable safeguards.



Further Information

Further information regarding the processing of supplier information can be found in:

- Data Protection Policy.
- Procurement and Financial Regulations.
- Records Management Policy.
- Supplier Due Diligence Procedures.
- Visitor Management Procedures.
- CCTV Policy.

These documents are available on the Trust website or upon request.



Section G: Visitors

Who This Section Applies To

This section applies to individuals visiting schools and premises operated by The Rose Learning Trust, including parents, carers, contractors, agency workers, professionals, guests, volunteers and other visitors attending Trust sites. It explains how the Trust collects, uses, stores and shares personal information relating to visitors.

Information We Collect

The Trust may collect, use, store and share personal information relating to visitors, including:

- Name.
- Company or organisation details.
- Telephone number.
- Email address.
- Vehicle registration number.
- Visitor arrival and departure information.
- Photographs captured as part of electronic visitor management systems.
- Visitor signatures recorded through sign-in systems.
- CCTV images captured on Trust premises.

The Trust uses both electronic and paper-based visitor management systems to record attendance on site. Electronic visitor sign-in systems are provided by Osborne Technologies.

Why We Use This Information

The Trust processes visitor information to:

- Protect the welfare and safeguarding of pupils.
- Maintain the security of school buildings and Trust premises.
- Protect Trust networks, systems and information assets.
- Ensure the health, safety and wellbeing of visitors.
- Manage site access and visitor identification.
- Support emergency evacuation and incident management procedures.
- Meet legal and regulatory obligations relating to safeguarding, security and data sharing.

How We Collect Information

Visitor information may be collected:

- Directly from visitors during sign-in procedures.
- Through electronic visitor management systems.
- Through paper-based visitor sign-in records.



- Through CCTV systems operating on Trust premises.
- During pre-arranged visits, meetings, events or contractor activities.

Who We Share Information With

The Trust will only share visitor information where there is a lawful basis to do so.

Where necessary, information may be shared with:

- Security organisations, where required to support the safety and welfare of pupils, staff and visitors.
- Emergency services, where required to respond to incidents, emergencies or health and safety concerns.
- Law enforcement agencies, courts or other public authorities where required by law.

Authorised personnel from Osborne Technologies may access visitor management systems where necessary to provide technical support and maintenance services.

Site Security and Safeguarding

Maintaining the safety and security of pupils, staff and visitors is a key responsibility of the Trust. Visitor information helps us:

- Verify the identity of individuals entering Trust premises.
- Manage safeguarding arrangements.
- Respond effectively in emergencies.
- Investigate incidents where necessary.
- Comply with health and safety requirements.

Where applicable, visitor information may be cross-referenced with safeguarding, visitor management or security procedures to ensure pupils and staff remain protected.

Storage and Retention

Visitor information is stored securely using approved electronic and paper-based systems. Electronic records may be stored locally within schools, on Trust systems, secure servers or approved cloud services. Paper records are held securely within Trust record management systems.

Visitor information is retained in accordance with the Trust's Records Management Policy and Retention Schedule. Information may be retained beyond a visit where necessary to comply with legal, safeguarding, health and safety or operational requirements.



Visitor Security Measures

The Trust implements appropriate technical and organisational measures to protect visitor information against unauthorised access, loss, alteration or disclosure. Access to visitor records is limited to authorised personnel who have a legitimate business need to access the information.

The Trust also maintains procedures for identifying, investigating and responding to suspected data breaches where required by law.

Further Information

Further information regarding the processing of visitor information can be found in:

- Data Protection Policy.
- Visitor Management Procedures.
- Safeguarding and Child Protection Policy.
- Health and Safety Policy.
- Records Management Policy.
- CCTV Policy.

These documents are available on the Trust website or upon request.

