THE ROSE LEARNING TRUST

DATA PROTECTION POLICY

Date	**September 2019**
Prepared by	**Central Team**
Review Date	**September 2020**
Version	**V1**

CONTENTS

1	**Aims**
2	**Legislation at glance**
3	**Definitions**
4	**The Data Controller**
5	**Roles and responsibilities**
6	**Data Protection principles**
7	**Collecting personal data**
8	**Sharing personal data**
9	**Biometric recognition systems**
10	**Subject access requests and other rights of individuals**
11	**Parental requests to see the education record**
12	**CCTV**
13	**Photographs and Videos**
14	**Data protection by design and default**
15	**Data security and storage**
16	**Disposal of records**
17	**Personal data breaches**
18	**Training**
19	**Monitoring arrangements**
20	**Links with other policies**

1 Aims

The Rose Learning Trust aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill. This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2 Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information. In addition, this policy complies with our funding agreement and articles of association

3 Definitions

TERM	DEFINITION
Personal Data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data, which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting,

	altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4 The data controller

The Rose Learning Trust processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller. The Rose Learning Trust is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to all staff employed by The Rose Learning Trust, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Trustees board

The board has overall responsibility for ensuring that complies with all relevant data protection obligations

5.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO. Full details of the DPO's responsibilities are set out in their job description.

Our DPO is Deborah Temperton and is contactable via DPO@roselearning.co.uk

5.3 Headteacher

The Headteacher acts as the representative of the data controller on a day-today basis

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address

Contacting the DPO in the following circumstances:

- With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
- If they have any concerns that this policy is not being followed
- If they are unsure whether they have a lawful basis to use personal data in a particular way
- If they need to rely on or capture consent, draft a privacy notice for something not already covered by an existing privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contacts or sharing data with third parties

6 Data Protection Principles

The GDPR is based on data protection principles that our school must comply with.
The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how The Rose Learning Trust aims to comply with these principles: -

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of six 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**

- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data
If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with our Records Management Policy.

8 Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
- Only appoint suppliers or contractors which can provide enough guarantees that they comply with data protection law
- Establish a data sharing agreement with the supplier or contractor, wither in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations

- Research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9 Biometric Recognition Systems

We do not currently use biometric recognition systems within our trust. An example would be to use fingerprints to receive school dinners instead of using an online payment system. We would comply with the requirement of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric system is put in place or before their child first takes part in it. The school will get written consent form at least one parent or carer before we take any biometric data from their child and first process this.

Parents/carers and pupils would have the right to choose not to use the school's biometric system. We would provide alternative means of accessing the relevant services for those pupils. For example, pupils could pay for school dinner using an online payment where available.

Parents/carers and pupils could withdraw consent at any time, and we would make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent give by the pupil's parent(s)/carer(s)

Where staff members of other adults would use the school's biometric system(s), we would also obtain their consent before they first take part in it and provide alternative means of accessing the relevant service. If they object staff and other adults could also withdraw consent at anytime and the school will delete any relevant data captured.

Note: that in the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18.

10 Subject access requests and other rights of individuals

10.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with?

- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Our Subject Access Request Policy and procedure sets out how individuals can make requests and how we will respond

10.2 Other data protection rights of the individuals

In addition to the right to make a subject access request, and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified based on public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

11 Parental requests to see the educational record

In England, Wales and Northern Ireland, the parent's right of access to their child's 'educational record' is only relevant in maintained schools, and not in academies.

Parents are only entitled to access information about their child by making a SAR if the child is unable to act on their own behalf or has given their consent.

12 CCTV

We use CCTV in various locations around our school sites within the Trust to ensure it remains safe. We will adhere to the ICO's Code of Practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the DPO.

13 Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our schools.

We will obtain consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

14 Data protection by design and default

We will put measures in place to show that we have integrated data protection into all our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant

Maintaining records of our processing activities, including:

For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)

For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

15 Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access

- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices. USB devise are discouraged in preference to online secure cloud storage such as Office 365
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment, for example email on mobile phones
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected

16 Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide enough guarantees that it complies with data protection law

17 Personal data breaches

The trust will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in our Data Breach Policy

18 Training

All staff, governors and volunteers are provided with data protection training as part of their induction process and no less than annually. More frequent training and briefings will be encouraged, to create a culture of data security and awareness, and where new guidance is introduced.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary

19 Monitoring arrangements

Trust central team have gained Cyber essentials award which will be rolled out to the trust schools during the academic year 2019-2020 and will monitor the success of all the schools in succeeding in acquiring this NCSC accreditation

- Trust working with the Information Security Consultant in working towards ISO27001
- Internal trust and LGB monitoring sheets the outcomes of which are subject to termly QA

The Trust purchases external services from:

- Data Protection & Compliance Solutions Limited (GDPR legal compliance)

- Secure Schools (Cyber security compliance software)
- Information Security Consultant (specialist in technical assurance/information assurance/ IT security controls and risk management)

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and shared with the full trust board

20 Links with other policies

This data protection policy is linked to the trust-wide policies below:

- Subject Access Request Policy
- Data Handling Procedures Policy
- Data Breach Policy
- Privacy Notices for pupils/parents, staff, Trustees/Governors/ Volunteers
- Safeguarding Policy