



## **DATA PROTECTION POLICY**

<b>Date Published</b>	<b>September 2019</b>
<b>Prepared by</b>	<b>Trust</b>
<b>Review date</b>	<b>2022</b>
<b>Review Cycle</b>	<b>Annual</b>
<b>Version</b>	<b>4</b>

## CONTENTS

<b>1</b>	<b>Introduction</b>
<b>2</b>	<b>Policy Objectives</b>
<b>3</b>	<b>Information Covered</b>
<b>4</b>	<b>Key Principles</b>
<b>5</b>	<b>Lawful Basis for processing personal information (Article 6 GDPR)</b>
<b>6</b>	<b>Data Protection Officer</b>
<b>7</b>	<b>Data Protection Impact Assessments (DPIA)</b>
<b>8</b>	<b>Documentation and Records</b>
<b>9</b>	<b>Data Minimisation</b>
<b>10</b>	<b>Individual Right and Responsibilities</b>
<b>11</b>	<b>Photographs and Electronic Images</b>
<b>12</b>	<b>Access to Personal Data</b>
<b>13</b>	<b>Security of Personal Data</b>
<b>14</b>	<b>Data Breaches</b>
<b>15</b>	<b>Complaints</b>
<b>16</b>	<b>Consequence of a failure to comply</b>
<b>17</b>	<b>Links to other policies</b>
<b>18</b>	<b>Review</b>
<b>19</b>	<b>Contacts</b>
<b>20</b>	<b>Glossary</b>

## **1 Introduction**

- 1.1 The Data Protection Act (DPA) 2018 and the General Data Protection Regulations (GDPR) provide the law which safeguards personal privacy, giving protection for individuals as to how their personal information is used. It applies to anyone who handles or has access to people's personal data.
- 1.2 Schools are required to have a data protection policy which must comply with the GDPR. This is because every school is classed as a Data Controller under the data protection legislation because they decide how personal data for which they are responsible is processed. Each school and every employee has a legal duty to protect the privacy of information relating to individuals that it processes.
- 1.3 The Information Commissioner as the Regulator can impose fines of up to 20 million Euros (approximately £17 million) for serious breaches of the GDPR, therefore it is imperative that the trust and all staff comply with the legislation.

The Rose Learning Trust (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 Policy Objectives**

- 2.1 This policy is intended to ensure that The Rose Learning Trust personal information is dealt with properly and securely and in accordance with the legislation. It will apply to personal information regardless of the way it is used, recorded, and stored and whether it is held in paper files or electronically.
- 2.2 The trust is committed to being concise, clear, and transparent about how it obtains and uses personal information and will ensure data subjects are aware of their rights under the legislation.
- 2.3 All staff must have a general understanding of the law and understand how it may affect their decisions in order to make an informed judgement about how information is gathered, used, and ultimately deleted. All members of staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines and shall attend regular training to ensure compliance with their responsibilities.

## **3 Information Covered**

- 3.1 Personal data is defined under the GDPR as "any information relating to an identifiable person who can be directly or indirectly identified by reference to an identifier held by the school."
- 3.2 The information includes factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of a living individual. This includes any expression of opinion about an individual and intentions towards an individual. Under the GDPR personal

information also includes an identifier such as a name, an identification number, location data or an online identifier.

- 3.3 The trust collects and uses a large amount of personal information every year about staff, pupils, parents, and other individuals who come into contact with the trust. By way of example, this includes pupil records, staff records, names, and addresses of those requesting prospectuses, test marks, references, and fee collection of Local Authorities (LAs), government agencies and other bodies. In addition, there may be a legal requirement for the trust to process personal information to ensure that it complies with statutory obligations.
- 3.4 The information collected is processed in order to enable the trust to provide education and other associated functions.

## **4 Key Principles**

- 4.1 Data Protection Principles – there are six enforceable principles contained in Article 5 of the General Data Protection Regulations, which the trust must adhere to when processing personal data.
- Principle 1 – Personal data shall be processed lawfully, fairly and in a transparent manner (lawfulness, fairness, and transparency)
  - Principle 2 – Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation)
  - Principle 3 – Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purpose(s) for which they are processed (data minimisation)
  - Principle 4 – Personal data shall be accurate and where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay. (accuracy)
  - Principle 5 - Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. (Storage limitation)
  - Principle 6 (the Security Principle) - Personal data shall be processed in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage to personal data, using appropriate technical or organisational measures (integrity and confidentiality)
- 4.2 There is a 7th Principle - the Accountability Principle which requires organisations to take responsibility for what they do with personal data and how they comply with the other principles. At the trust, the responsibility for adherence to the principles lies with all trust staff.

- 4.3 The organisation must have appropriate measures and records in place to be able to demonstrate their compliance.
- 4.4 In addition to adherence to the principles, there are transfer limitations relating to the transfer of personal data to a country outside the EEA. Should an occasion arise requiring such a transfer, members of staff should contact the Data Protection Officer for assistance.
- 4.5 Overall commitment to compliance with the above principles.
- 4.6 Alongside actions relating to specific obligations with which the legislation obliges the trust to comply, and which are included below in relevant sections of this Policy, the trust will:
- a. Produce an information asset register that contains details of the records it holds.
  - b. Inform individuals why the information is being collected at the point it is collected by way of privacy notices.
  - c. Inform individuals when their information is shared, and why and with whom it will be shared.
  - d. Check the quality and the accuracy of the information it holds.
  - e. Ensure that information is not retained for longer than is necessary.
  - f. Ensure that when obsolete, information is destroyed, and it is done so appropriately and securely.
  - g. Create, maintain, and publish a Disposal and Retention Schedule setting out retention and disposal dates for common data sets and other information.
  - h. Ensure that clear and robust safeguards are in place to protect personal information from loss, theft, and unauthorised disclosure, irrespective of the format in which it is recorded.
  - i. Share information with others only when it is fair and lawful to do so and satisfies the lawful basis for processing that information (lawful bases are set out in §5.0).
  - j. Share personal data with other organisations for the purpose of crime prevention and/or detection, or for the purpose of legal proceedings, provided that the disclosure falls within an exemption to the non-disclosure provisions contained within the Data Protection Act 1998 or any subsequent legislation.
  - k. Disclose personal data where required to do so by law for example, following receipt of a court order.
  - l. Set out procedures to ensure compliance with the duty to respond to an individual's rights to:
    - request access to personal information, known as Subject Access Requests.
    - be informed about the way their data is used.
    - have inaccurate personal data rectified.

- have their personal data erased.
  - restrict the processing of their personal data; and
  - object to the processing of their personal data.
- m. Ensure the trust staff are appropriately and regularly trained and aware of and understand the trust's policies and procedures.
- n. Create and maintain a data breach notification spreadsheet to record data breaches and also in circumstances where a breach was narrowly avoided
- o. Automated Decision Making  
If the trust carries out automated decision making (including profiling), comply with all the relevant requirements of the GDPR.

#### **4.7 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 given 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 any time 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.

### **5. Lawful Basis for processing personal information (Article 6 GDPR)**

- 5.1 Before any processing activity starts for the first time, and then regularly afterwards, the purpose(s) for the processing activity and the most appropriate lawful basis (or bases) for that processing, must be selected by the trust

5.2 The lawful basis for processing which has been selected must be recorded, to demonstrate compliance with the data protection principles, and include information about the purpose of the processing and the justification for why you believe this basis applies.

5.3 The lawful bases:

- The data subject has given consent to the processing of his or her data for one or more specific purposes. (Consent)
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. (Contract)
- Processing is necessary for compliance with a legal obligation to which the data controller is subject. (Legal Obligation)
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person. (Vital interests)
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the school (Public Task)
- Processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. (Legitimate Interests) N.B. This basis does not apply to processing carried out by public authorities in the performance of their tasks. However, the ICO indicates that where there are other legitimate purposes outside the scope of the tasks as a public authority, legitimate interests may be considered where appropriate.

5.4 Where the lawful basis for processing is consent this must be clearly evidenced by a very clear and specific statement. Such consent requires a positive opt-in and so pre-ticked boxes, or any other method of default consent will not be sufficient. If consent is given in a document which deals with other matters, the consent must be kept separate from those other matters

The data subject shall have the right to withdraw his or her consent at any time and withdrawal must be promptly honoured. Prior to giving consent, the data subject shall be notified of the right of withdrawal.

## **5.5 Processing of special categories of personal data – Article 9**

5.5.1 Processing of sensitive personal information is prohibited unless a lawful special condition for processing is identified. It comprises data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life or orientation or which concerns health or is genetic or biometric data which uniquely identifies a natural person.

5.5.2 Such personal data will only be processed by the trust if:

- a. There is a lawful basis for doing so as identified in Article 6.
- b. One of the special conditions for processing sensitive personal information applies:
  - (i) the individual ('data subject') has given explicit consent (which has been clearly explained in a Privacy Notice)
  - (ii) the processing is necessary for the purposes of exercising the employment law rights or obligations of the school or the data subject
  - (iii) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent
  - (iv) the processing is carried out during its legitimate activities with appropriate safeguards by a foundation, association, or any other not-for-profit body with a political, philosophical, religious or trade-union aim
  - (v) the processing relates to personal data which are manifestly made public by the data subject
  - (vi) the processing is necessary for the establishment, exercise, or defence of legal claims
  - (vii) the processing is necessary for reasons of substantial public interest
  - (viii) the processing is necessary for purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, the provision of social care and the management of social care systems or services
  - (ix) the processing is necessary for reasons of public interest in the area of public health.
- c. The trust's privacy notice(s) set out the types of sensitive personal information that it processes, what it is used for, the lawful basis for the processing and the special condition that applies.

5.6 Sensitive personal information will not be processed until an assessment has been made of the proposed processing as to whether it complies with the criteria above and the individual has been informed (by way of a privacy notice or consent) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

5.7 Unless the trust can rely on another legal basis of processing, explicit consent is usually required for processing sensitive personal data. In such circumstances the trust will obtain evidence of and record consent so that it can demonstrate compliance with the GDPR.

## **6 Data Protection Officer (DPO)**

6.1 The DPO cannot hold a position that requires them to determine the purpose and means of processing personal data, for example, the Head Teacher, or Head of Information Technology. Our appointed DPO is:

Name: Deborah Temperton  
Address: The Rose Learning Trust  
Central Office  
Stevens Road  
Doncaster  
DN4 0LT

Telephone: 07730217963  
Email: [DPO@roselearning.co.uk](mailto:DPO@roselearning.co.uk)

## 7 Data Protection Impact Assessments (DPIA)

- 7.1 The trust will carry out a DPIA when processing is likely to result in high risk to the data protection rights and freedoms of individuals
- 7.2 The GDPR does not define high risk, but guidance highlights a number of factors that are likely to trigger the need for a DPIA, which include:
- 7.2.1 the use of new technologies,
  - 7.2.2 processing on a large scale,
  - 7.2.3 systematic monitoring,
  - 7.2.4 processing of special categories of personal data.
- 7.3 The purpose of the DPIA is to assess:
- 7.3.1 whether the processing is necessary and proportionate in relation to its purpose
  - 7.3.2 the risks to individuals, including both the likelihood and the severity of any impact on them
  - 7.3.3 what measures can be put in place to address those risks and protect personal information.
- 7.4 Staff should adhere to the Data Protection Toolkit for Schools from the DfE with reference to the DPIA template. When carrying out a DPIA they should seek the advice of the DPO for support and guidance and once complete, refer the finalised document to the DPO for sign off.

## 8 Documentation and 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 devices are discouraged in preference to online secure cloud storage such as Office 365

- 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

8.1 The trust in accordance with its duty as a Data Controller and Data Processor will keep detailed records of data processing activities and the records shall contain: -

- a. the name and contact details of the trust and, if applicable, of any joint controllers,
- b. the name and contact details of the trust's Data Protection Officer
- c. the name and details of individuals or roles that carry out the processing
- d. the purposes of the processing
- e. a description of the categories of individuals i.e., the different types of people whose personal data is processed
- f. categories of personal data processed.
- g. categories of recipients of personal data
- h. details of any transfers to third countries, including documentation of the transfer mechanism safeguards in place
- i. retention schedules
- j. a description of technical and organisational security measures

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

8.2 The trust will make these records available to the Information Commissioner's Office (ICO) upon request and will, on an annual basis, provide its registrable particulars and pay the data protection fee to the ICO.

8.3 As part of the trust's record of processing activities the DPO will document, or link to documentation on:

- a. information required for privacy notices such as:
- b. the lawful basis for the processing
- c. the legitimate interests for the processing
- d. individuals' rights
- e. the source of the personal data
- f. records of consent
- g. controller-processor contracts
- h. the location of personal data
- i. DPIA reports and
- j. records of personal data breaches

8.4 Records of processing of sensitive information are kept on:

- a. the relevant purposes for which the processing takes place, including why it is necessary for that purpose
- b. the lawful basis for the processing and
- c. whether the personal information is retained or has been erased in accordance with the Retention Schedule and, if not, the reasons for not following the policy.

8.5 The trust will conduct regular reviews of the personal information it processes and update its documentation accordingly. This may include:

- a. Carrying out information audits to find out what personal information is held
- b. Talking to staff about their processing activities
- c. Reviewing policies, procedures, contracts, and agreements to address retention, security, and data sharing.

## **9 Privacy Notices**

9.1 A privacy notice under the GDPR should include:

- The trust's name and contact details
- The contact details of the DPO.
- The personal data you are collecting & why you are collecting it.
- Where you get the personal data from & who you are sharing it with.
- The lawful basis for processing the data
- How long the data will be held for.
- Transfers to third countries and safeguards.
- Description of the data subjects' individual rights.
- The data subjects right to withdraw consent for the processing of their data.
- How individuals can complain.

9.2 The trust will publish an overarching privacy notice, which will be posted on its website, which will provide information about how and why the trust gathers and uses images and shares personal data.

9.3 In addition to publication of that notice, the trust will also issue privacy notices, to all parents and pupils, before, or as soon as possible after, any personal data relating to them is obtained. This may simply be an explanation of why the information is being requested and the purpose for which it will be used.

9.4 The trust will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible, and easily accessible form, using clear and plain language.

9.5 The trust will issue a minimum of two privacy notices, one for pupil information, and one for workforce information, and these will be reviewed at regular intervals to ensure they reflect current processing and are in line with any statutory or contractual changes

9.6 The privacy notices will be amended to reflect any changes to the way the trust processes personal data.

9.7 The privacy notice will include details of how/ if the trust uses CCTV (if applicable), whether it intends to use biometric data and how consent will be requested to do this and include details of the trust's policy regarding photographs and electronic images of pupils.

## **10 Data Minimisation**

**10.1 The trust will ensure that personal data**

- Is only collected for the specified, explicit, and legitimate purposes
- Is not further processed in any manner incompatible with those purposes

- Is no used for new, different, or incompatible purposes from that disclosed when it was first obtained unless the data subject has been informed of the new purposes and they have consented where necessary

## **10.2 Data minimisation**

- Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
- Staff may only process data when their role requires it. Staff will not process personal data for any reason unrelated to their role.
- The trust maintains a Retention Schedule to ensure personal data is deleted after a reasonable time for the purpose for which it was being held unless a law requires such data to be kept for a minimum time.
- Staff will take all reasonable steps to destroy or delete all personal data that is held in its systems when it is no longer required in accordance with the Schedule. This includes requiring third parties to delete such data where applicable.
- The trust will ensure that data subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

## **11 Individual Rights and Responsibilities**

### **11.1 Individual rights**

The trust will observe the following rights which staff as well as any other 'data subjects' enjoy in relation to their personal information:

- To be informed about how, why and on what basis that information is processed (see the relevant privacy notice)
- To obtain confirmation that personal information is being processed and to obtain access to it and certain other information, by making a subject access request
- To have data corrected if it is inaccurate or incomplete
- To have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing ('the right to be forgotten')
- To restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but the individual(s) concerned does/do not want the data to be erased) or where the trust no longer needs the personal information, but the individual(s) require(s) the data to establish, exercise or defend a legal claim
- To restrict the processing of personal information temporarily where they do not think it is accurate (and the trust is verifying whether it is accurate), or where they have objected to the processing (and the trust is considering whether the trust's legitimate grounds override the individual's(s') interests)
- In limited circumstances to receive or ask for their personal data to be transferred to a third party in a structured, commonly used, and machine-readable format
- To withdraw consent to processing at any time (if applicable)
- To request a copy of an agreement under which personal data is transferred outside of the EEA.

- To object to decisions based solely on automated processing, including profiling
- To be notified of a data breach which is likely to result in high risk to their rights and obligations
- To make a complaint to the ICO or a Court.

## 11.2 Individual Responsibilities

During their employment, staff may have access to the personal information of other members of staff, suppliers, clients, or the public. The trust expects staff to help meet its data protection obligations to those individuals.

If members of staff have access to personal information, they must:

- only access the personal information that they have authority to access and only for authorised purposes
- only allow other staff to access personal information if they have appropriate authorisation
- only allow individuals who are not trust staff to access personal information if they have specific authority to do so
- keep personal information secure (e.g., by complying with rules on access to premises, computer access, password protection and secure file storage and destruction in accordance with the trust's policies).
- not remove personal information, or devices containing personal information (or which can be used to access it) from the trust's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device
- not store personal information on local drives or on personal devices that are used for work purposes.

## 12 Photographs and Electronic Images

### 12.1 CCTV

The trust uses CCTV in various locations around the to ensure it remains safe. The trust will adhere to the ICO's Code of Practice for the use of CCTV.

There is no requirement to ask individuals' permission to use CCTV, but the trust to 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.

### 12.2 Photographs and Videos

As part of the trust's activities, we, or a 3<sup>rd</sup> party (e.g., school photographers) may want to take photographs and record images of individuals within the school.

The trust will obtain **written** 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.

Uses may include:

- Within trust schools on notice boards and in trust magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our trust/school websites or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

### **13 Access to Personal Data**

#### **13.1 This section sets out the process that will be followed by the trust when responding to requests for access to personal data made by the pupil or their parent or carer with parental responsibility.**

There are two distinct rights of access to information held by schools about pupils, parents/carers, and staff:

- Pupils and parents or those with Parental Responsibility have a right to make a request under the GDPR to access the personal information held about them.
- Pupils and parents or those with Parental Responsibility have a right to access the educational records. The right of those entitled to have access to curricular and educational records is defined within the Education (Pupil Information) (England) Regulations 2005.

#### **13.2 Handling a subject access request for access to personal data:**

13.2.1 Article 15 of the GDPR gives individuals the right to access personal data relating to them, processed by a data controller. The right can be exercised by a person with Parental Responsibility on behalf of their child dependent on the age and the understanding of the child. For the purposes of a subject access request the trust will apply the full legal definition of 'Parental Responsibility' when determining who can access a child's personal data

13.2.2 Requests for information may come in from various sources whether verbally, through webforms/social networks or in writing, which can include e-mail, to any member of staff. Where possible the requestor should be encouraged to complete a request form to best capture what information is being requested. If the original request does not clearly identify the information required, then the trust will seek further enquiries to clarify what information is being requested.

13.2.3 The request will be recorded within the GDPRiS portal and assigned to a member of staff to monitor and ensure the request is investigated and either fulfilled or rejected.

13.2.4 The identity of the requestor must be established before the disclosure of any information is made. Proof of the relationship with the child (if not known) must also be established as this will verify whether the individual making the request can lawfully exercise that right on behalf of the child.

Below are some examples of documents which can be used to establish identity:

- Passport
- Driving licence

- Utility bill with current address
- Birth/marriage certificate
- P45/P60
- Credit card or mortgage statement

13.2.5 It is widely accepted that children of primary school age do not have the maturity to understand and exercise their own rights and as such it is acceptable for those with Parental Responsibility to exercise these rights on their child's behalf. However, each request will be considered on its own merits and the circumstances surrounding the request and the child. A child with competency to understand can refuse to consent to a request for their personal information made under the GDPR. This position differs when the request is for access to the Education Record of the child (see below for more detail).

13.2.6 No charge can be made for access to personal data that is not contained within an education record, but the trust reserves the right to cover its communication costs e.g., photocopying, postage, in which case a fees notice will be sent to the requestor

13.2.7 The response time for a subject access request is **1 calendar month** from the date of receipt

13.2.8 The relevant response time period for a subject access request will not commence until any necessary clarification of information has been sought and received from the requestor. The time to respond can be extended to two months where the request is complex or numerous.

13.2.9 There are some exemptions available under the Data Protection Act which will mean that occasionally personal data will need to be redacted (information blacked Data Protection Policy May 2018 out/removed) or withheld from the disclosure. All information will be reviewed prior to disclosure to ensure that the intended disclosure complies with the trust's legal obligations.

13.2.10 Where the personal data also relates to another individual who can be identified from the information, the information will be redacted to remove the information that identifies the third party. If it is not possible to separate the information relating to the third party from the information relating to the subject of the request, consideration will be given to withholding the information from disclosure. These considerations can be complex and additional advice will be sought when necessary.

13.2.11 Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil, or another person will be withheld along with any information that would reveal that the child is at risk of abuse, or information relating to Court Proceedings.

13.2.12 Where redaction has taken place then a full copy of the information provide will be retained in order to maintain a record of what was redacted and why and a clear explanation of any redactions will be provided in the trust's response to the request

13.2.13 If there are concerns about the disclosure of information additional advice will be sought

### **13.3 Handling a request for access to a curricular and educational record as defined within the Education (Pupil Information) (England) Regulations 2005**

- 13.3.1 A parent may make a request to access information contained within their child's education record, regardless of whether the child agrees to the disclosure of information to them. The right of access belongs to the parent in these cases. It is not a right being exercised by the parent on behalf of the child.
- 13.3.2 For the purpose of responding to an Educational Records request, the trust will apply the definition of 'parent' contained within the Education Act 1996
- 13.3.3 An "education record" means any record of information which: -
- a. Is processed by or on behalf of the trust board/LGB or a teacher within the trust
  - b. Relates to any person who is or has been a pupil within the trust; and
  - c. Originated from or was supplied by or on behalf of the persons specified in paragraph (a), other than information which is processed by a teacher solely for the teacher's own use
- 13.3.4 The amount that can be charged for a copy of information contained in an education record will depend upon the number of pages provided. The charge made will be in accordance with the Education (Pupil Information) (England) Regulations 2005.
- 13.3.5 No charge will be made to view the education record
- 13.3.6 The response time for requests made under the Education (Pupil Information) (England) Regulations 2005 is 15 school days (this does not include half terms or teacher training days) or 1 calendar month, whichever is shorter
- 13.3.7 An exemption from the obligation to comply with the request will be claimed where the disclosure of the information to the parent may cause serious harm to the physical or mental or emotional condition of the pupil or another person or if the disclosure of the information would reveal that the child is at risk of abuse

## **14 Retention and Disposal of Data**

The trust board will ensure that the trust has a up to date and accurate retention and disposal schedule that is compliant with GDPR. The trust will ensure that personal data is stored, transferred, and disposed of securely and in accordance with the retention and disposal schedule.

## **15 Security of personal data**

- 15.1 The Security Principle requires that appropriate security is put in place to prevent the personal data it holds being accidentally or deliberately compromised.
- 15.2 In order to comply with this principle the trust will: -
- Ensure that all individuals involved in processing data understand the requirements of confidentiality, integrity and availability for the personal data being processed.
  - Undertake an analysis of the risks presented by its processing, and uses this to assess the appropriate level of security it needs to put in place to keep paper and electronic personal data secure and ensure that appropriate security measures are enforced
  - Ensure that only authorised individuals have access to personal data.
  - Put in place appropriate physical and organisational security measures, as well as technical measures, and regularly review the physical security of the trust buildings and storage systems.

- Require staff to ensure that no personal data will be left unattended in any vehicles and that if it is necessary to take personal data from trust premises, for example to complete work from home, the data is suitably secured.
- Review its information security policy regularly and takes steps to make sure the policy is implemented.
- Put in place basic technical controls and be aware that it may also need to put other technical measures in place depending on the circumstances and the type of personal data it processes
- Use encryption and/or pseudonymisation where it is appropriate to do so.
- Ensure that all portable electronic devices containing personal data are password protected.
- Refer to any relevant guidance and seek advice where necessary if processing personal data utilising a cloud-based solution.
- Make sure that it can restore access to personal data in the event of any incidents, such as by establishing an appropriate backup process.
- Ensure that any data processor it uses also implements appropriate technical and organisational measures.

15.3 The trust will conduct regular testing and reviews of its measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement

## **16 Data Breaches**

16.1 A data breach may take many different forms:

- Loss or theft of data or equipment on which personal information is stored
- Unauthorised access to or use of personal information either by a member of staff or third party
- Loss of data resulting from an equipment or systems (including hardware or software) failure
- Human error, such as accidental deletion or alteration of data
- Unforeseen circumstances, such as a fire or flood
- Deliberate attacks on IT systems, such as hacking, viruses or phishing scams
- Blagging offences where information is obtained by deceiving the organisation which holds it

16.2 In the event of the loss, damage, or theft of equipment:

- notification of the loss, damage or theft of any equipment should be sent at the first opportunity to the DPO, with any details of personal data that may have been affected.
- a written or e-mail report must be filed within 24 hours to the Head Teacher and nominated Data Protection Lead.
- the employee responsible for that equipment will describe to their management the circumstances surrounding the loss, damage, or theft.
- The DPO and Head Teacher will provide guidance as to notice to be provided to the appropriate police authorities.

16.3 The trust will require staff, in the event of a data breach however caused, and whether or not it occurs on a school working day, in term time or school holiday time, to ensure they inform the DPO and Head Teacher, or in their absence Senior Leaders, immediately that the

breach is discovered and make all reasonable efforts to recover the information, following the trust's agreed breach reporting process

- 16.4 In the event of a data breach occurring the trust will comply with the requirement to report the breach to the DPO without undue delay and the DPO will determine whether there is a requirement to report such breach to the Information Commissioner's Office, on the basis that it is likely to result in a risk to the rights and freedoms of individuals. The trust is required to report such a breach within 72 hours of discovery. The trust will also notify the affected individuals if the breach is likely to result in such a high risk

## **17 Complaints**

- 17.1 Subject to paragraphs 17.2 and 17.3, complaints relating to the trust's compliance with the GDPR will be dealt with in accordance with the trust's Complaints Policy.
- 17.2 Complaints relating to access to personal information or access to education records should be made to our DPO (see section 4 of this policy) who will decide whether it is appropriate for the complaint to be dealt with through the trusts' complaints procedure. Complaints which are not appropriate to be dealt with through the trust's complaints procedure can be referred to the Information Commissioner. Details of how to make a complaint to the ICO will be provided with the response letter.
- 17.3 Complaints relating to information handling may be referred to the Information Commissioner's Office (the statutory regulator). Contact details can be found on their website at [www.ico.org.uk](http://www.ico.org.uk) or telephone 01625 5457453

## **18 Consequences of a failure to comply**

- 18.1 The trust takes compliance with this policy very seriously. Failure to comply puts data subjects whose personal information is being processed at risk and 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.
- 18.2 Any failure to comply with any part of this policy may lead to disciplinary action under the trust's procedures and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

## **19 Links to other policies**

This Policy should be read in conjunction with the following policies:

Anti-Malware Policy
Biometric Recognition Systems
Child Friendly Privacy Notice
Data Handling and Lawful basis for processing
Data Protection/GDPR
Data Retention
DFE Information Sharing Policy

Disposal of Assets Policy
DPIA
Firewalling Policy
ICO Certificate 2020-2021
ICO Model publication scheme Freedom of Information Act
ICO Registration Details
Images and Video
IT Acceptable Use
Password Policy
Patch Management Policy
Privacy Notice - Job applications
Privacy Notice - Trustees/Governors/Volunteers
Privacy Notice for Coronavirus Track and Trace
Privacy Notice for Covid-19 Testing of staff in primary school
Privacy Notices for pupil, parents, and carers
Privacy notices for staff
Publication Scheme and Freedom of Information
Ransomware Policy
Records Management & Retention Schedule
Records Management Annex 1
Subject Access Request
Surveillance and CCTV Policy
Whistleblowing

## 20 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

- 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)

## 21 Review

This policy will be reviewed annually for the next two years to ensure any further guidance issued by the ICO is reflected within the policy, and thereafter every three years, or sooner if statutory requirements change

## 22 Contacts

Any enquiries in relation to this policy should be directed to Deborah Temperton –  
Deborah.temperton@roselearning.co.uk

## 22 Glossary

**Automated Decision-Making (ADM):** when a decision is made which is based solely on automated processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits automated decision-making (unless certain conditions are met) but not automated processing.

**Automated Processing:** any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location, or movements. profiling is an example of automated processing.

**Consent:** agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, which signifies agreement to the processing of personal data relating to them.

**Data Controller:** The natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. It is responsible for establishing practices and policies in line with the GDPR. The school is the Data Controller of all personal data relating to its pupils, parents, and staff.

**Data Subject:** a living, identified or identifiable individual about whom we hold personal data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their personal data.

**Data Privacy Impact Assessment (DPIA):** tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major systems or business change programs involving the processing of personal data.

**Data Protection Officer (DPO):** the person required to be appointed in public authorities under the GDPR.

**EEA:** the 28 countries in the EU, and Iceland, Liechtenstein, and Norway.

**Explicit Consent:** consent which requires a very clear and specific statement (not just action).

**General Data Protection Regulation (GDPR):** General Data Protection Regulation ((EU) 2016/679). Personal data is subject to the legal safeguards specified in the GDPR.

**Personal data:** Any information relating to an identified or identifiable natural person (data subject) who can be identified, directly or indirectly by reference to an identifier such as a name, 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 includes sensitive personal data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location, or date of birth) or an opinion about that person's actions or behaviour.

**Personal data breach:** A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

**Privacy by Design:** implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

**Privacy Notices:** separate notices setting out information that may be provided to Data Subjects when the school collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, school workforce privacy policy) or they may be stand-alone privacy statements covering processing related to a specific purpose.

**Processing:** Anything done with personal data, such as collection, recording, structuring, storage, adaptation or alteration, retrieval, use, disclosure, dissemination or otherwise making available, restriction, erasure, or destruction.

**Processor:** A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the data controller.

**Pseudonymisation or Pseudonymised:** replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

**School Day:** Any day in which there is a session and pupils are in attendance.

**Sensitive Personal Data:** information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal data relating to criminal offences and convictions.

**Working Days:** Exclude school holidays and "inset" or training days where the pupils are not present.