General Data Protection Regulation

(Non-Statutory)

Approved: Summer 2022
Date of Next Review: Summer 2024

Equality Impact Assessment - Policy Review
In reviewing this policy, we have tried to make a positive impact on equality by considering and reducing or removing inequalities and barriers which already existed. We have ensured that this policy does not impact negatively on the dimensions of equality.

This policy is to let you know how The Roseland Multi Academy Trust ('the Trust') will collect, use and process personal data. It is also designed to let you know your rights and what you can do if you have questions about personal data.

The Trust is the controller for the purposes of data protection laws.

This document sets out the types of personal data (meaning information about an individual from which that individual can be personally identified) we handle, the purposes of handling those personal data and any recipients of it.

Our Details
We are The Roseland Multi Academy Trust
Registered Company Number: 07557817
Address: Tregony, Truro, Cornwall, TR2 5SE
Information Commissioner's Office Registration Number: ZA170029
Our Data Protection Officer is: Mr Richard Clarke and their contact details are: rclarke@theroseland.co.uk

Why We Collect Data
We collect and hold personal information relating to our students and may also receive information about them from their previous schools, the Local Authority, Department for Education (DfE) and other bodies linked to their education, development and welfare. We may also share personal data with other agencies as necessary under our legal duties or otherwise in accordance with our duties/obligations as schools.

Whilst the majority of student information we are provided with or collect is mandatory, some of it is provided to us on a voluntary basis. We will inform you whether you are required to provide certain student information to us or if you have a choice in this.

Below are set out the reasons why we collect and process personal data, as well as the legal basis on which we carry out this processing:

- **to support our students' learning**: we will process personal data to help every child achieve his or her potential in all areas of learning and to promote excellence in our teaching and learning environment.
- **monitor and report on their progress**: we will process personal data to record students' progress to help set and monitor targets and boost achievements and aspirations of all students.
- **provide appropriate pastoral care**: we will process personal data to ensure that all students are properly supported in their time with us. We will process data to help staff understand and respond to the unique circumstances of all students.
- **assess the quality of our services**: we will process personal data so that we may reflect on our own practices to help us improve and provide the highest quality education that we can to all students.
- **to ensure proper management of school trips and afterschool clubs and activities**: when students and parents participate in school trips and afterschool clubs and activities personal data will need to be processed.
- **to promote and protect health and safety**: in order to protect students, parents and staff in their involvement at the schools, we must process personal data relating to matters such as incidents and responses to incidents.

- **for employment purposes**: to assist in the running of the Trust and to enable individuals to be paid, we will process personal data of those employed to teach or otherwise engaged to work at the Trust.

Legal Basis for Processing

The lawful basis for us to collect/process this personal data is in order to provide education in accordance with statute law (such as the Education Act 1996 and other legislation), our funding agreements with the Secretary of State, our memorandum and articles of association and other guidance provided for in law.

In addition, personal data will be collected and/or processed for the purposes of relevant contracts for the provision of services which are paid for. This may include but is not limited to:

- the provision of music tuition;
- school trips;
- entering students for examinations.

We do not process any special categories of personal data except where necessary for reasons of substantial public interest in complying with legal obligations including under the Equality Act 2010 or where necessary to protect the vital interests of the data subject or of another natural person and where safeguards are in place to ensure that this personal data is kept secure. For the avoidance of doubt where special categories of personal data are collected it shall not be used for the purposes of automated decision making and/or profiling.

Special categories of data means personal data revealing:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs or trade union membership;
- genetic or biometric data that uniquely identifies you;
- data concerning your health, sex life or sexual orientation; or
- data relating to criminal convictions or offences or related security measures.

Further personal data including special categories of personal data may be collected and/or processed where consent has been given (for example, school photographs for non-educational purposes). If consent has been given, then this may be revoked in which case the personal data will no longer collected/processed.

Categories of Information We Collect

We may collect the following types of personal data (please note this list does not include every type of personal data and may be updated from time to time):

- contact details;
- date of birth;
- health and/or other medical information;
- information in connection with education (included but not limited to unique student numbers, test results, post-16 learning information and other records);
- attendance information;
- behavioural and disciplinary information;
- free school meal eligibility;
- information received in connection with any complaint;
- information required for employment purposes, such as:

    - national Insurance numbers;
    - remuneration details;
    - qualifications.
- personal characteristics of students, such as:
    - their nationality and ethnic group;
    - their religion;
    - their first-language;
    - any special educational needs they may have;
    - any relevant protected characteristics.

Who Will Have Access to Your Data

Personal data will be accessible by members of staff. Where necessary, volunteers and trustees will also have access to personal data.

We will not share information about our students with third parties without consent unless we are required to do so by law or our policies. We will disclose personal data to third parties:

- if we are under a duty to disclose or share your personal data in order to comply with any legal obligation; for example, we share students' personal data with the Department for Education on a statutory basis;
- in order to enforce any agreements with you;
- to protect the rights, property, or safety of the Trust, the schools, other students or others. This includes exchanging information with other organisations for the purposes of child welfare. This may include our Local Authority, the Department for Education, the Police and other organisations where necessary; for example, for the purposes of organising a school trip or otherwise enabling students to access services or for the purposes of examination entry. Information may also be sent to other schools where necessary; for example, schools that students attend after leaving us.

How Data Will Be Processed

Personal data may be processed in a variety of ways; this will include but is not limited to:

- sending by email;
- adding to spreadsheets, word documents or similar for the purposes of assessing personal data;
- for educational software use (this could be for the purposes of helping children learn, discipline, reports and other educational purposes).

Where we Store Data and How We Keep Data Secure

Paper copies of personal data are kept securely at each school; for example, in secure filing cabinets.

Electronic copies of personal data are kept securely and information will only be processed where we are satisfied that it is reasonably secure.

All information you provide to us is stored on secure servers. Where we have given you (or where you have chosen) a password which enables you to access certain parts of our website, you are responsible for keeping this password confidential. You must not share your password with anyone.

When giving personal data to third parties (for example, software providers) it is possible that this personal data could be stored in a location outside of the European Economic Area. We will take all steps reasonably necessary to ensure that your personal data is treated securely and in accordance with this privacy policy. In particular, any transfer of your personal data made by us to a location outside of the EEA will be governed by clauses in a written contract in order to keep these secure.

Retention Periods

We will only retain personal data for as long as is necessary to achieve the purposes for which they were originally collected, plus any statutory timeframes. As a general rule, personal data will be kept for the entire period that a child is a student at a school, with a further retention period of date of birth of the student plus 25 years. Other records (for example, safeguarding or in relation to special educational needs) will be kept for longer in accordance statutory guidance. Further information on retention periods can be obtained by contacting us via the details on Page 2.

Your Data Rights

The General Data Protection Regulation and associated law gives you rights in relation to personal data held about you and your child. These are:

- **Right of Access**: if your personal data is held by the Trust, you are entitled to access your personal data (unless an exception applies) by submitting a written request. We will aim respond to that request within one month. If responding to your request will take longer than a month, or we consider that an exception applies, then we will let you know. You are entitled to access the personal data described in "Requesting Your Data".
- **Right of Rectification**: you have the right to require us to rectify any inaccurate personal data we hold about you. You also have the right to have incomplete personal data we hold about you completed. If you have any concerns about the accuracy of personal data that we hold then please contact us.
- **Right to Restriction**: you have the right to restrict the manner in which we can process personal data where:
    - the accuracy of the personal data is being contested by you;
    - the processing of your personal data is unlawful, but you do not want the relevant personal data to be erased; or
    - we no longer need to process your personal data for the agreed purposes, but you want to preserve your personal data for the establishment, exercise or defence of legal claims.
    - Where any exercise by you of your right to restriction determines that our processing of particular personal data is to be restricted, we will then only process the relevant personal data in accordance with your consent and, in addition, for storage purposes and for the purpose of legal claims.
- **Right to Erasure**: You have the right to require we erase your personal data which we are processing where <u>one</u> of the following grounds applies:
    - the processing is no longer necessary in relation to the purposes for which your personal data were collected or otherwise processed;
    - our processing of your personal data is based on your consent, you have subsequently withdrawn that consent and there is no other legal ground we can use to process your personal data;
    - the personal data have been unlawfully processed; and
    - the erasure is required for compliance with a law to which we are subject.
- **Right to Data Portability**: you have the right to receive your personal data in a format that can be transferred. We will normally supply personal data in the form of emails or other

mainstream software files. If you want to receive your personal data which you have provided to us in a structured, commonly used and machine-readable format, please contact us via the details on Page 2.

The Trust may refuse to respond to a request if it is manifestly unfounded or excessive or may charge a reasonable fee for dealing with the request. If your request is manifestly unfounded or excessive, the Trust will demonstrate why.

You can find out more about the way these rights work from the website of the Information Commissioner's Office (ICO).

Requesting Your Data (Subject Access Requests)
Individuals have a right to make a 'subject access request' to gain access to personal information that the Trust 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 is not 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.

Subject access requests must be submitted in writing, either by letter, email or fax to the Data Protection Officer. They should include:

- name of individual;
- correspondence address;
- contact number and email address;
- details of the information requested;
- if staff receive a subject access request they must immediately forward it to the Data Protection Officer.

Children and Subject Access Requests
Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students in our Trust may not be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

Responding to Subject Access Requests
When responding to requests, we:

- may ask the individual to provide 2 forms of identification;

- may contact the individual via telephone to confirm the request was made;
- will respond without delay and within 1 month of receipt of the request;
- will provide the information free of charge;
- may tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary.

We will not disclose information if it:

- might cause serious harm to the physical or mental health of the student or another individual;
- would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests;
- is contained in adoption or parental order records;
- is given to a court in proceedings concerning the child;
- if the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs;
- a request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the Information Commissioner's Office.

Biometric Recognition Systems

Where we use students' biometric data as part of an automated biometric recognition system (for example, students use finger prints to receive school dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.

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

Parents/carers and students have the right to choose not to use the Trust's biometric system(s). We will provide alternative means of accessing the relevant services for those students.

Parents/carers and students can object to participation in the Trust's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a student 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 student's parent(s)/carer(s).

Where staff members or other adults use the Trust's biometric system(s), we will 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 can also withdraw consent at any time, and the Trust will delete any relevant data already captured.

CCTV

We use CCTV in various locations around the Trust sites to ensure they remain 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 Data Protection Officer.

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

We will obtain written consent from parents/carers, or students aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and student. Where we do not need parental consent, we will clearly explain to the student how the photograph and/or video will be used.

Uses may include:
- within school/Trust on notice boards, brochures, newsletters, etc;
- outside of school/Trust by external agencies such as the school photographer, newspapers, campaigns;
- online on our school/Trust websites and 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.

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;
- where personal information needs to be taken off site, staff must sign it in and out from their school office;
- 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 students 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;
- 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.

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 Trust's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Making a Complaint

If you are unhappy with the way we have dealt with any of your concerns, you can make a complaint to the ICO, the supervisory authority for data protection issues in England and Wales. We would recommend that you complain to us in the first instance, but if you wish to contact the ICO on the details you can do so on the details below. The ICO is a wholly independent regulator established in order to enforce data protection law.

ICO Concerns website: www.ico.org.uk/concerns
ICO Helpline: 0303 123 1113
ICO Email: casework@ico.org.uk
ICO Postal Address: Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

Changes to this Policy

Any changes we make to this policy in the future will be posted on our websites and, where appropriate, notified to you by email. Please check back frequently to see any updates or changes.