# DATA PROTECTION POLICY

| | |
|---|---|
| **Trust/Governor Lead:** | **Director/HR** |
| **Status & Review Cycle:** | **Statutory** |
| **Nominated Lead Member of Staff:** | **Executive Head/Headteacher/CFOO/Head of IT Operations** |
| **Last Review Date:** | **September 2026** |
| **Next Review Date:** | **September 2028** |

**Contents**

1. Aims ..... 3
2. Legislation and guidance ..... 3
3. Definitions ..... 3
4. The data controller ..... 4
5. Roles and responsibilities ..... 4
6. Data protection principles ..... 5
7. Collecting personal data ..... 6
8. Sharing personal data ..... 7
9. other rights of individuals ..... 7
10. Parental requests to see the educational record ..... 8
11. Photographs and videos ..... 8
12. Data protection by design and default ..... 8
13. Data security and storage of records ..... 9
14. Disposal of records ..... 10
15. Training ..... 10
16. Monitoring arrangements ..... 10
17. Links with other policies ..... 10

## 1. Aims

The 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 UK General Data Protection Regulation (UK-GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018).

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 UK-GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the UK-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. Also, see our CCTV Policy.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

## 3. Definitions

| Term | Definition |
|---|---|
| **Personal data** | Any information relating to an identified, or identifiable, individual.<br><br>This may include the individual's:<br>• Name (including initials)<br>• Identification number<br>• Location data<br>• Online identifier, such as a username<br><br>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:<br>• Racial or ethnic origin<br>• Political opinions<br>• Religious or philosophical beliefs<br>• Trade union membership<br>• Genetics<br>• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes |

| | |
|---|---|
| | • Health – physical or mental<br>• 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.<br>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 Trust processes personal data relating to parents, pupils, staff, Governors, visitors and others, and therefore is a data controller.

The School 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 our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

**5.1** The Trust Board has overall responsibility for ensuring that the Schools within the Trust comply with all relevant data protection obligations.

**5.1 Governing Board**

The Governing Board of each school has specific responsibility for ensuring that the School 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 Trust 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

Danielle Eadie of RADCaT Ltd and is contactable via:

T: 01942 590 785 | E: Danielle.eadie@radcat.co.uk

**5.3 Headteacher**

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

**5.4 All Staff**

Staff within Trust schools 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 or If they are unsure whether or not 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, deal with data protection rights invoked by an individual, or transfer personal data outside the United Kingdom. o If there has been a data breach.
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals o If they need help with any contracts or sharing personal data with third parties.

**6. Data Protection Principles**

The UK-GDPR is based on data protection principles that Trust schools 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 Trust and its schools aim 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 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the Trust/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 Trust/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 Trust/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 Trust/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 UK-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).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

**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 the Trust's/school's UK-GDPR Record 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 sufficient guarantees that they comply with data protection law.
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share.
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

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 situation that affects any of our pupils or staff.

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

## 9. Other Rights of Individuals

### 9.1 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), 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 on the basis of public interest.
- Request a copy of agreements under which their personal data is transferred outside of the United Kingdom.

- 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.

**10. Parental Requests to see the Educational Record**

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

**11. Photographs and Videos**

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

We 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 school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the School photographer, newspapers, campaigns.
- Online on our school website 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.

See our Safeguarding policy for more information on our use of photographs and videos.

**12. CCTV**

We use CCTV in various locations around some of our school sites 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. Please refer to each school's CCTV policy for further information.

Any enquiries about the individual CCTV systems should be directed to the Data Protection Officer (DPO).

**13. Biometric Data**

The Trust will comply with the 'Protection of Freedoms Act' (2012) when processing biometric data; written consent will be sought from at least one parent or legal guardian of pupils under the age of 18 prior to any processing taking place.

Clear information on the use of biometric systems to access school services must be provided to pupils and parents allowing them to make an informed choice about participation. Please refer to the 'Biometric Data Policy' for further information.

**14. Data Protection by Design and Default**

We will put measures in place to show that we have integrated data protection into all of 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 (see section 6).
- Completing privacy impact assessments where the Trust's/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 Trusts 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.

**13. 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 safe 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 the 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 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.
- 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 (see our acceptable use policy).
- 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 (see section 8).

**NB: Also, see our UK-GDPR Data Records Management Policy.**

**14. 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 sufficient guarantees that it complies with data protection law.

**15. Training**

All staff and Governors are provided with data protection training as part of their induction process.

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

**16. Monitoring Arrangements**

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if a fundamental change in legislation occurs, after the introduction of DPA 2018 or UK-GDPR 2016. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the Trust Board and the governing bodies of Trust schools.

**17. Links with Other Policies**

This data protection policy is linked to our:

- Freedom of Information Policy
- Freedom of Information Publication Scheme
- ICT Acceptable Use Policy
- Safeguarding Policy

This Policy will be reviewed on a bi-annual basis.

Adopted by the Trust Board in October 2021 and reviewed in Spring 2024

Review date: Spring 2026