Raedwald Trust

connection learning without exception resilience respect

Data Protection Policy

Policy Details	
Person Responsible for this Policy	**Angela Ransby**
Policy Author	**Angela Ransby**
Date to Trust Board	**October 2024**
Date Ratified	**13th November 2024**
Review Date	**November 2025**
Policy displayed on website	**YES**

CEO Signature	**Angela Ransby**
Trust Board Signature	**Alan Whittaker**

Updates Made	Date
p. 5, section 6 – updated reference to data protection legislation	October 2024
Section 8, Subject Access Requests updated and appendix 1 (Subject Access Request Form) removed	April 2025

Contents

1. Aims

Our Trust aims to ensure that all data collected about staff, pupils, parents and visitors is collected, stored and processed in accordance with data protection legislation.

This policy sets out how we seek to protect personal data and to ensure that trust personnel understand the rules governing their use of the Personal Data they have access to in the course of their work.

Any breach of this Data Protection Policy may result in disciplinary action. Substantial or intentional breaches of this policy, such as accessing personal data without authorisation or a legitimate reason, may constitute gross misconduct and could lead to dismissal without notice.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and Guidance

Data protection legislation includes the Data Protection Act 2018 which incorporates the UK General Data Protection Regulation (UK GDPR), the Privacy and Electronic Communications (EC Directive) Regulations 2003 and any legislation implemented in connection with the General Data Protection Regulation which is the governing legislation that regulates data protection across the EEA.

This policy meets the requirements of, and is based on guidance published by the Information Commissioner's Office and model privacy notices published by the Department for Education.

This policy complies with our funding agreement and articles of association.

3. Definitions

Term	Definition
Personal data	Data from which a person can be identified, Either from that data alone or in combination with other identifiers we possess or can reasonably access. 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.
Special categories of personal data	Personal data which is more sensitive and so needs more protection. Data such as: • Racial or ethnic origin • Political opinions • Religious beliefs, or beliefs of a similar nature • Where a person is a member of a trade union • Genetics • Biometrics (eg. Fingerprints) used for identification purposes • Physical and mental health • Sex life or sexual orientation • Data relating to criminal convictions We treat FSM, SEN and safeguarding data as

	special category data in accordance with best practice recommendations.
Processing	Collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.
Data subject	The person whose personal data is held or processed
Data controller	A person or organisation that determines the purposes and the means of processing personal data
Data processor	A person or organisation who processes personal data on behalf of the data controller. This can be a member of staff, 3rd party company or another organisation.
Trust personnel	All employees, workers contractors, agency workers, consultants, directors and members.
Personal data breach	Personal data that has been accidentally or unlawfully lost, stolen, destroyed, altered, disclosed or made available where it should not have been.
Privacy notice	A privacy notice helps people understand how their data is used. It includes information on the personal data held, the purpose for holding it and who the data is shared with. It also provides information on individuals rights in respect of their data.
Subject access request (SAR)	Individuals have the right to access the data held about them. We have to provide the data requested within one calendar month of the request.

4. The Data Controller

Our Trust processes personal information relating to pupils, staff and visitors, and therefore is a data controller. The Trust is registered as a data controller with the Information Commissioner's Office and renews this registration annually.

5. Data Protection Principles

The Raedwald Trust shall comply with the principles of the UK General Data Protection Regulations (UK GDPR). The UK GDPR states 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 we aim to comply with these principles.

5.1 Lawfulness, fairness and transparency

We will only process personal data where we have a lawful basis (legal reason) to do so. Under data protection law there are 6 lawful bases (listed in order of relevance):

- Public task: processing is necessary so we can carry out our official functions
- Legal obligation: the processing is necessary so we can comply with the law.
- Contract: processing is necessary to fulfil a contract with the individual, or because they have asked the school to take specific steps before entering into a contract
- Consent: the individual (or their parent/carer when appropriate) has freely given clear consent
- Vital interests: the processing is necessary to protect someone's life
- Legitimate interests: *not applicable to public authorities.*

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.

5.2 Purpose and limitation

We will collect personal data for specified, explicit and legitimate reasons. We explain the data we collect, the purpose and lawful basis for collection in our privacy notices.

5.3 Accuracy and retention

We will endeavour to ensure that the data we store is accurate and up to date.

For long term placements we undertake an annual exercise to check the data we hold is correct (e.g. name, address, phone number, next of kin details, emergency contact and other essential information). This exercise also provides individuals with the opportunity to review the consent they have given for the school.

Parents/carers and staff are also requested to inform the school when their personal information changes.

We retain data in accordance with our retention schedule published on the Raedwald Trust website - https://www.raedwaldtrust.com/about-raedwald-trust/data-protection/

6. Roles and Responsibilities

The Trust board has overall responsibility for ensuring that the Trust complies with its obligations under data protection legislation. The board of trustees and management are responsible for ensuring all Trust Personnel comply with this Data Protection Policy and are responsible for implementing appropriate practices, processes, controls and training to ensure such compliance.

The Chief Financial Officer is responsible for day to day implementation of this policy.

The Head Teacher has day-to-day responsibility in each academy, or the deputy in their absence. The Head Teacher will ensure that all staff are aware of their data protection obligations, and oversee any queries related to the storing or processing of personal data.

All staff are responsible for:

a) Ensuring that they comply with the Trust's IT and Communications Systems Policy (found in the Staff Handbook) and that:
   - 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 are not left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access;
   - Personal data is not in the view of others when being used;

- Computer screens are locked when unattended;
- Personal data is only held on the trust network or a trust issued device (laptop, USB memory stick or other removable media) which is encrypted, password protected, kept in a locked location when not in use;
- Passwords are not shared;
- Passwords comply with the complexity requirements, are changed regularly and different passwords are used for separate systems and devices. A unique password must be used for email accounts;
- Personal data is only shared where necessary and in accordance with trust policy, internally by sending a link to a document on the network, externally using encrypted email;
- Personal data is not disclosed accidentally or otherwise, to any unauthorised third party;
- Personal data is securely disposed of when it is no longer required and in accordance with the document retention schedule.
- Where personal information needs to be taken off site (in paper or electronic form), it is signed out and in from the school office.

b) Ensuring that they only access data that they have authority to access and only for authorised purposes;

c) Informing the Chief Financial Officer of any changes to their personal data, such as a change of name, address, or updated relevant medical circumstances;

d) Contacting the Chief Financial Officer if they:
- receive a Subject Access Request
- have questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
- have any concerns that this policy is not being followed
- are engaging in a new activity that involves personal data
- need help with any contracts or sharing personal data with third parties.

e) Notifying the Chief Financial Officer immediately in the event of discovering a data breach.

As a public body, we are required to appoint a Data Protection Officer (DPO). The DPO role is fulfilled by Tracey Riches, Clear 7 Consultancy.

The role of the DPO is to:
- Inform and advise the Trust and the employees about obligations to comply with all relevant data protection laws.
- Monitor compliance with the relevant data protection laws.
- Be the first point of contact for supervisory authorities.
- Coordinate training on data protection for all key stakeholders.

7. Privacy/Fair Processing Notice

Our privacy notices explain the types of personal data we collect, why we hold it and who we share it with. It also explains how we'll store and handle that data and keep it safe.

Our privacy notices can be found on the Raedwald Trust website - https://www.raedwaldtrust.com/about-raedwald-trust/data-protection/

8. Subject Access Requests

Individuals have a right to make a 'subject access request' to request a copy of the personal information that we hold about them. To help individuals exercise this right, the Information Commissioners' Office has an online form: Make your subject access request | ICO.

We ask that Subject Access Requests (SARs) are made using this form so that we can ensure that we provide the information you would like. However SARs can also be made verbally or by letter or email.

9. Disposal of Records

Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely in accordance with our Retention Schedule which can be found on the Raedwald Trust website - https://www.raedwaldtrust.com/about-raedwald-trust/data-protection/

Paper-based records will be shredded or held securely until it is safely disposed of using a specialist supplier. Electronic files will be deleted and we will use a specialist supplier to safely dispose of obsolete electronic equipment.

10. Photographs and videos

As part of the admission process we will ask for written consent from parents/carers to allow the photography of pupils and the specific use of these images, for example:

- 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, unless we have permission to do so, to ensure they cannot be identified.

11. CCTV

We use closed circuit television (CCTV) images to reduce crime and monitor the school buildings in order to provide a safe and secure environment for pupils, staff and visitors, and to prevent loss or damage to the school property. The Trust has a CCTV policy in place which documents:

- why CCTV is used
- where cameras are sited
- whether covert monitoring is undertaken
- how long images are retained for
- who has access to the images.

12. 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
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third- party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

13. Personal data breaches

Despite our best endeavours a data security breach could still happen. Examples include:

- Human error (eg. sending an email to the wrong person/s, sharing individual's email addresses by not using Bcc., posting information to the wrong address, dropping/leaving paperwork containing personal data in a public space)
- Loss or theft of equipment containing personal data (eg. Laptop, USB stick, mobile phone). Note this is a breach even if the device is encrypted.
- Equipment failure
- Fire, flood
- Hacking attack
- "Blagging" offences where personal data is obtained by deceit.

On finding or causing a breach, or potential breach, the Chief Financial Officer must notify the Data Protection Officer and complete the Data Breach template on the secure portal within 24 hours of discovery to enable compliance with the requirement to notify the regulator of high risk breaches within 72 hours.

Guided by the Data Protection Officer, the Chief Financial Officer will;

- Alert the CEO and the Chair of Trustees
- Make all reasonable efforts to contain and minimize the impact of the breach, assisted by the relevant staff members or data processors where necessary
- Document the breach and related decisions
- Capture lessons learned to evaluate how the breach occurred, the success of the response and any improvements to policies and processes to avoid the situation from happening again

The Data Protection Officer will;

- Assess the potential consequences, based on how serious they are and how likely they are to happen
- Decide whether the data subject needs to be notified of the breach
- Decide whether the breach must be reported to the ICO and if so, will notify the ICO within 72 hours of the breach being identified

14. Training

All staff and other key stakeholders (eg. Trustees, volunteers) will be made aware of their responsibilities for data protection as part of their induction programme.

Refresher training will take place annually. A central training record will be maintained.

15. Monitoring Arrangements

The Chief Financial Officer is responsible for monitoring and reviewing this policy.

This document will be reviewed annually. At every review, the policy will be shared with the Trust Board for ratification.

16. Links with other Policies

This Data Protection Policy is linked to:

- The freedom of information publication scheme
- IT and Communications Systems Policy (found in the RT Staff Handbook)
- CCTV Policy
- Retention Schedule (available on the RT website)