DATA PROTECTION & PRIVACY POLICY

RÆDWALD T·R·U·S·T

RATIFIED BY THE TRUST BOARD IN:
FEBRUARY 2019

NEXT REVIEW DATE: SEPTEMBER 2019

DATA PROTECTION & PRIVACY POLICY

Person responsible for this policy:	Angela Ransby
Policy author:	Angela Ransby
Date to Trust Board:	January 2019
Date Ratified:	
Date to be Reviewed:	September 2019
Policy displayed on website:	Yes

CEO Signature:	Angela Ransby
Trust Board Signature:	Roger Fern

TABLE OF 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 General Data Protection Regulation (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.

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.
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 General Data Protection Regulations (GDPR). The 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 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 Data Retention schedule (Appendix 2).

6. Roles and Responsibilities

The Trust board has overall responsibility for ensuring that the Trust complies with its obligations under the Data Protection Act 2018. 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 Trust Business Manager is responsible for day to day implementation of this policy.
The Head of School has day-to-day responsibility in each centre, or the deputy in their absence. The Head of School 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;
   - 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 Trust Business Manager of any changes to their personal data, such as a change of name, address, or updated relevant medical circumstances;
d) Contacting the Trust Business Manager 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 Trust Business Manager 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 as follows:
Pupils and parents
Staff

8. Subject Access Requests

Individuals have a right to make a Subject Access Request (SAR) to request a copy of the personal information that we hold about them.

To help individuals exercise this right we provide a Subject Access Request form on our website. Hard copies of the form can be requested from each centre's reception. We ask that SARs are made using the form so that we can ensure that we provide the information requested however subject access requests can also be made verbally or by letter or email.

We will generally respond to SARs within one calendar month. There is no charge for a SAR.
If staff receive a SAR request they must immediately forward it to the Trust Business Manager.
Appendix 1 provides more information about SARs.

9. Parental Requests to see the Educational Record

Parents, or those with parental responsibility, may request access to their child's educational record, which will be provided at the discretion of the Headteacher within 15 school days of receipt of a written request.

10. 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 Document Retention Schedule (Appendix 2).

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.

11. 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.

12. 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 school 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.

13. 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.

14. 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 staff member or data processor must notify the Trust Business Manager immediately.

More information on personal data breaches can be found in our Personal Data Breach Procedure.

15. Training

All staff and other key stakeholders (eg. governors, 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.

16. Monitoring Arrangements

The Trust Business Manager 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.

17. Links with other Policies

This data protection policy is linked to:
the freedom of information publication scheme.
IT and Communications Systems Policy
CCTV policy

Appendix 1: 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.

We provide a form to help individuals exercise this right. Hard copies of the form can be requested from the school reception. Subject access requests can also be made verbally or by letter or email. If staff receive a subject access request they must immediately forward it to the DPO.

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 in respect of their child we consider whether the child is mature enough to understand their rights.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, subject access requests from parents or carers of pupils may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis. Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. The Gillick competency guidelines would be applied to this understanding. In this instance, subject access requests from parents or carers of pupils may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

On receipt of a SAR we may ask for 2 forms of identification, for example a passport and utility bill. We will also:

- confirm the request in writing and our understanding of the information requested
- respond without delay and within 1 month of receipt. Where a request is complex or numerous we may extend this to 3 months. We will confirm this within 1 month, and explain why the extension is necessary

In certain circumstances we may not disclose information. When we refuse a request, we will explain why, and provide information on how to complain to the Information Commissioners Office.

There is generally no charge for a SAR. However, if the request is considered to be 'manifestly unfounded or excessive' we may charge an administration fee or refuse to provide the information. A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.
We maintain a register of SARs received to enable us to monitor this.

Subject Access Request Form

This form is intended to support individuals with their requests for personal data and to help us ensure that we provide the information that is being requested.

1. Whose data is being requested?	
Name	
Address	
Relationship with the school For example: Pupil, employee, governor, parent, volunteer	
2. Who is making the request?	
Name	
Address (if different from above)	
Telephone	
Email	
Are you requesting your own data? If yes, go to Section 3	Yes/No
If no, what is your relationship with the person whose data is being requested?	
3. What information is being requested?	
Are you looking for anything specific? For example: • Your personnel file • Your child's medical records • Your child's behaviour record • Emails between 'A' and 'B' between [date]	
Is there a particular time period you are interested in?	
Is there anyone specific we should talk to?	

How would you like the information to be provided? For example: email, verbally, by post	
Signed:	
Date:	

Please forward to Sharon Williets swilliets@raedwaldtrust.org or Natalie Quinton nquinton@raedwaldtrust.org Trust Business Managers.

Appendix 2: Document retention schedule

Our Document Retention Schedule can be found on our website.

Personal data breach procedure

A personal data breach is '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.'

In other words, personal data has that been accidentally or unlawfully:

- Lost,
- Stolen,
- Destroyed,
- Altered,
- Disclosed or made available where it should not have been.

On finding or causing a breach, or potential breach, the Trust Business Manager must notify the Data Protection Officer using the Data Breach template below within 24 hours of discovery to enable compliance with the requirement to notify the regulator of high risk breaches within 72 hours.

The Data Protection Officer will:

- alert the headteacher and the chair of governors
- make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.
- 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.
- 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.

Pupils and Parents PRIVACY NOTICE

Introduction

This Privacy Notice explains the types of personal data we may collect about you, 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.
The Raedwald Trust is registered under the General Data Protection Regulations 2018 as a data controller.
Our Data Protection Officer is Tracey Riches, Clear 7 Consultancy.

What types of personal data do we collect?

The categories of pupil information that we collect include:

- Personal information: including name, DOB and address
- Characteristics: including ethnicity, language, nationality, country of birth and free school meal eligibility
- Attendance information: including frequency and reason for absence
- Assessment information
- Health information: including medical conditions and information regarding SEND
- Behavioural information, including temporary exclusions
- Photos and video recordings, CCTV footage
- Safeguarding information

Why we hold your personal data

We collect and use the pupil data to:

- Meet legal requirements
- Meet our statutory obligations to safeguard and protect children and vulnerable people
- Enable effective learning
- Manage behaviour
- Review our effectiveness
- Keep pupils, parents and carers informed.

Explaining the legal bases we rely on

We only collect and use pupils' personal data when the law allows us to. Generally, we process it to:

- Comply with a legal obligation
- Perform an official task in the public interest

We may also process pupils' personal data in situations where we:

- Have obtained consent to use it in a certain way
- Need to protect the individual's vital interests (or someone else's interests)

Where we have obtained consent to use pupils' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

How long will we keep your personal data?

We only keep your data for as long as is necessary for the purpose for which it was collected.

Timescales are detailed in our document retention policy. At the end of that retention period, your data will either be deleted completely or anonymised so that it can be used for statistical analysis and business planning.

Who do we share your personal data with?

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.

We routinely share pupil information with:

- schools that pupils attend after leaving us
- other places where the pupil is receiving education such as colleges or home tuition
- our local authority
- the Department for Education (DfE)
- support services where the sharing of data is in the best interests of the pupil

The Department for Education has legal powers to collect the pupil, child and workforce data that schools, local authorities and awarding bodies hold. For more information about the department's data sharing process, please visit:
https:/www.gov.uk/data-protection-how-we-collect-and-share-research-data

To contact the department: https:/www.gov.uk/contact-dfe

Where your personal data may be processed

The trust will not transfer your data to countries outside the European Economic (EEA).

What are your rights over your personal data?

You have the right to:

- Request access to the personal data we hold about you, free of charge in most cases. This is known as a Subject Access Request. To help you exercise this right we provide a form on our website. Hard copies of the form can be requested from the school reception. We ask that SARs are made using the form so that we can ensure that we provide the information requested however subject access requests can also be made verbally or by letter or email.
- The correction of your personal data when incorrect, out of date or incomplete.
- Require the school to delete or stop processing your data, for example where the data is no longer necessary for the purpose of processing.
- Object to the processing of your data where the school is relying on its legitimate interests as the legal ground for processing.
- Withdraw consent. Whenever you have given us your consent to use your personal data, you have the right to change your mind at any time and withdraw that consent.

If we are not able to action your request we will explain to you the reasons why.

Security

Data security is of great importance to the trust and to protect your data we have put in place suitable physical, electronic and managerial procedures to safeguard and secure your collected data.

We take security measures to protect your information including:

- Limiting access to our buildings to those that we believe are entitled to be there (by use of passes, key card access and other related technologies);
- Implementing role based access controls to our information technology
- Use of appropriate procedures and technical security measures (including strict encryption, anonymisation and archiving techniques) to safeguard your information across all our computer systems, networks, websites, mobile apps and offices.

Contacting the Regulator

If you feel that your data has not been handled correctly, or you are unhappy with our response to any requests you have made to us regarding the use of your personal data, you have the right to lodge a complaint with the Information Commissioner's Office. We hope that you would consider raising any issue or complaint you have with us first and we will try to resolve any problems that you may have.

The Information Commissioner's Office can be contacted by calling 0303 123 1113.
Or go online to www.ico.org.uk/concerns

Any questions?

We hope this Privacy Notice has been helpful in explaining how we handle your personal data and your rights to control it.

If you have any questions, please contact our Data Protection Officer who will be pleased to help you:
Email us at swilliets@raedwaldtrust.org or nquinton@raedwaldtrust.org
Or write to us at Raedwald Trust, c/o First Base Ipswich, Raeburn Road, Ipswich IP3 0EW
This notice was last updated in January 2019.

EMPLOYEE PRIVACY NOTICE

Introduction

This Privacy Notice explains in detail the types of personal data we may collect about you, why we hold it and who we share it with.
The Raedwald Trust is registered under the General Data Protection Regulations 2018 as a data controller.
Our Data Protection Officer is Tracey Riches, Clear 7 Consultancy.

What types of personal data do we collect?

The categories of employee information we collect include:

- Personal information: including name, address and national insurance number
- Special categories of data: including gender, ethnicity, sexual orientation, religion or belief and trade union membership
- Recruitment data: Qualifications, skills, experience and employment history, nationality and entitlement to work in the UK, criminal record details;
- Health information
- Contract information: including working patterns, salary, annual leave, pension and benefits information;
- Payroll information: including bank details
- Performance management information: including appraisals, disciplinary or grievance procedures and related correspondence;
- Absence data: including the reasons for absence;
- CCTV footage.

Why we hold your personal data

We collect and use employee data to:

- Comply with statutory, regulatory, and contractual obligations
- Inform our recruitment and retention policies
- Enable individuals to be paid
- Support the effective performance management of staff
- Enable effective financial modelling and planning
- To have an emergency contact in case of need
- To give support if the need arises if absent from work.

Explaining the legal bases we rely on

The law on data protection sets out a number of different reasons for which an organisation may collect and process your personal data, including:

- Contract: We need your personal information to enter into an employment contract with you and to meet our obligations as employer. For example to pay you and to administer your entitlements.
- Legal obligation: We are required to check your entitlement to work in the UK, to deduct tax, to comply with health and safety laws and to enable you to take the leave you are entitled to.
- Consent: In specific situations, we may ask your consent to process your data.

How long will we keep your personal data?

We only keep it for as long as is necessary for the purpose for which it was collected.
Timescales are detailed in our document retention policy. At the end of that retention period, your data will either be deleted completely or anonymised so that it can be used for statistical analysis and business planning.

Who do we share your personal data with?
We do not share information about our employees with anyone without consent unless the law and our policies allow us to do so.

We share employee information as part of the recruitment process including references and Disclosure and Baring Service checks.

We also share information with:

- our local authority
- the Department for Education (DfE)
- our payroll provider School's Choice
- our HR provider School's Choice
- our occupational health provider School's Choice

We are required to share information about our employees with our local authority (LA) under section 5 of the Education (supply of information about the school workforce) (England) Regulations 2007 and amendments.

The Department for Education has legal powers to collect the pupil, child and workforce data that schools, local authorities and awarding bodies hold. For more information about the department's data sharing process, please visit:
https:/www.gov.uk/data-protection-how-we-collect-and-share-research-data

To contact the department: https:/www.gov.uk/contact-dfe

Where your personal data may be processed

The school will not transfer your data to countries outside the European Economic (EEA).

You have the right to:

- Request access to the personal data we hold about you, free of charge in most cases.
- The correction of your personal data when incorrect, out of date or incomplete.
- Require the school to delete or stop processing your data, for example where the data is no longer necessary for the purpose of processing
- Object to the processing of your data where the school is relying on its legitimate interests as the legal ground for processing
- Withdraw consent. Whenever you have given us your consent to use your personal data, you have the right to change your mind at any time and withdraw that consent.

If we are not able to action your request we will explain to you the reasons why.

Contacting the Regulator

If you feel that your data has not been handled correctly, or you are unhappy with our response to any requests you have made to us regarding the use of your personal data, you have the right to lodge a complaint with the Information Commissioner's Office.
You can contact them by calling 0303 123 1113.
Or go online to www.ico.org.uk/concerns

Any questions?

We hope this Privacy Notice has been helpful in explaining how we handle your personal data and your rights to control it.

If you have any questions that haven't been covered, please contact our Data Protection Officer who will be pleased to help you:
Email us at swilliets@raedwaldtrust.org or nquinton@raedwaldtrust.org
Or write to us at Raedwald Trust, c/o First Base Ipswich, Raeburn Road, Ipswich IP3 0EW
This notice was last updated in January 2019.