THE RISE TRUST

DATA PROTECTION POLICY

Record of updates

DATA PROTECTION POLICY

Date Created	July 2008
Adopted by Trustees	July 2009
Revision Due	July 2010
Reviewed	July 2011
Reviewed	July 2012
Revision Due	July 2013
Revision Due	July 2014
Revision Due	July 2015
Revision Due	February 2016
Revision Due	February 2017
Revision Due	April 2018 ready for GDPR
Revision Due	March 2019 – checked by DPO
Revision Due	March 2020

DOCUMENT VERSION CONTROL		
Issue No.	Issue Date	Summary of Changes
1	July 2008	Original Draft Policy
2	July 2009	Reviewed
3	July 2010	Reviewed
4	July 2011	Reviewed
5	July 2012	Reviewed
6	July 2013	Wording change
7	July 2014	Wording change
8	October 2015	Subject Access Request letter
9	February 2016	Addition of audit information and Appendices E & F
10	February 2017	Updated Appendix F & G
11	December 2017	Added Clean desk policy Appendix 7 (appendices now numbered)
12	Sept 2018	Drafted to be GDPR compliant
13	March 2019	Agreed with DPO
14	June 2020	Updated Children, Young people and Families Privacy notice

THE RISE TRUST DATA PROTECTION POLICY

Contents

1. Aims

Our organisation aims to ensure that all personal data collected about staff, children, parents, trustees, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.
This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the 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.
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. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username 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: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • 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. 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.
Pseudonymised	means the process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable individual;

4. The data controller

The RISE Trust processes personal data relating to job applicants and about current and former employees, temporary and agency workers, parents, children, contractors, interns, trustees, visitors, volunteers and apprentices for a number specific lawful purposes, as set out in The RISE Trust's Privacy Notices – Appendices 1-3..

Lynn Evans, C.E.O is responsible for data protection compliance within the Company. The organisation is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

We will review and update this policy in accordance with our data protection obligations. We will circulate any new or modified policy to staff when it is adopted.

5. Roles and responsibilities

This policy applies to **all staff** employed by our organisation, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Trustees

Trustees have overall responsibility for ensuring that our organisation 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 Trustee board and, where relevant, report to the board their advice and recommendations on organisation data protection issues.

The DPO is also the first point of contact for individuals whose data the organisation processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO company is One-West and is contactable via www.onewest.co.uk 01225 477944

5.3 CEO

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

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the organisation 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
    - 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 European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The GDPR is based on data protection principles that our organisation 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 and take reasonable steps to ensure that inaccurate personal information is deleted or corrected without delay;
- 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 organisation aims 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 organisation can **fulfil a contract** with the individual, or the individual has asked the organisation to take specific steps before entering into a contract
- The data needs to be processed so that the organisation 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 organisation, 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 organisation 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 GDPR and Data Protection Act 2018.

If we offer online services to children or parents, such as classroom apps and 'Tapestry', and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

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.

The RISE Trust has three privacy notices:

1) For employees and volunteers (appendix 1)

2) For children, young people and families (appendix 2)

3) For contractors (appendix 3) – we will also include a supplier agreement letter with this (appendix 9)

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 fulfil their role.

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 **The RISE Trust retention schedule and Core recording policy.**

8. Sharing personal data

We will not normally share sensitive personal data with anyone else, but may do so where:

- There is an issue with a child 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 children – 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 children or staff.

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

The RISE Trust will not carry out automated decision-making (including profiling) based on any individual's sensitive personal information.

9. Recruitment and employment

During the recruitment process: the HR department, with guidance from Lynn Evans, C.E.O, will ensure that (except where the law permits otherwise):

a) during the short-listing, interview and decision-making stages, no questions are asked relating to sensitive personal information, eg race or ethnic origin, trade union membership or health;

b) if sensitive personal information is received, eg the applicant provides it without being asked for it within his or her CV or during the interview, no record is kept of it and any reference to it is immediately deleted or redacted;

c) any completed equal opportunities monitoring form is kept separate from the individual's application form, and not be seen by the person shortlisting, interviewing or making the recruitment decision;

d) 'right to work' checks are carried out before an offer of employment is made unconditional, and not during the earlier short-listing, interview or decision-making stages;

e) we will only ask health questions once an offer of employment has been made.

1.2 **During employment**: the HR department, with guidance from Lynn Evans, C.E.O, will process:

a) health information for the purposes of administering sick pay, keeping sickness absence records, monitoring staff attendance and facilitating employment-related health and sickness benefits;

b) sensitive personal information for the purposes of equal opportunities monitoring and pay equality reporting. Where possible, this information will be anonymised; and

c) trade union membership information for the purposes of staff administration and administering 'check off'.

10. Subject access requests and other rights of individuals

Individual rights

10.1 You (in common with other data subjects) have the following rights in relation to your personal information. Hyperlinks to the relevant ICO information is included:

a) to be informed about how, why and on what basis that information is processed—see The RISE Trust's Privacy Notices (Appendices 1-3)

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/ ;

b) to obtain confirmation that your information is being processed and to obtain access to it and certain other information, by making a subject access request (see Appendix 4) -https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/ ;

c) to have data corrected if it is inaccurate or incomplete https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-rectification/ ;

d) to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as 'the right to be forgotten') https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/ ;

e) to restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased), or where the employer no longer needs the personal information but you require the data to establish, exercise or defend a legal claim https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-restrict-processing/ ; and

f) to restrict the processing of personal information temporarily where you do not think it is accurate (and the employer is verifying whether it is accurate), or where you have objected to the processing (and the employer is considering whether the organisation's legitimate grounds override your interests) https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/ .

10.2 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the organisation 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 isn't 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 DPO (appendix 5). 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 DPO.

10.3 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 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, most subject access requests from parents or carers of children at our organisation 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.

10.4 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 phone 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 child 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 ICO.

10.5 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 European Economic Area
- 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.

11. 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 28 organisation days of receipt of a written request.

12. Photographs and videos

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

The RISE Trust will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

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

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 (see section 6)
- Completing data privacy impact assessments (DPIAs) where the organisation'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 organisation 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. 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 desks, tables, pinned to notice/display boards, or left anywhere else where there is general access (see Clear Desk Policy appendix 7)
- Where personal information needs to be taken off site, staff must ensure it is in a secure receptacle and not left unattended in a car
- Passwords must follow the RISE Trust guidance – passwords to have letters, capitals, punctuation and numbers (see The RISE Trust IT policy)
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, children or trustees who store personal information on their personal devices are expected to follow the same security procedures as for organisation-owned equipment (see The RISE Trust IT 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)
- Staff should follow The RISE Trust's Records Retention policy – see Appendix 6, which sets out the relevant retention period.

15. Disposal of records

We will conduct regular reviews of the personal information we process and update our documentation accordingly. This may include:

a) carrying out information audits to find out what personal information The RISE Trust holds;

b) distributing questionnaires and talking to staff across The RISE Trust to get a more complete picture of our processing activities; and

c) reviewing our policies, procedures, contracts and agreements to address areas such as retention, security and data sharing.

d) documenting our processing activities in electronic form so we can add, remove and amend information easily.

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 cross shred paper-based records, and overwrite or delete electronic files. Any data to be shredded will be locked away until it can be

disposed of securely. We may also use a third party to safely dispose of records on the organisation's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

16. Data breaches

The organisation will make all reasonable endeavours to ensure that there are no personal data breaches.
In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 8.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a organisation context may include, but are not limited to:

- A non-anonymised dataset being published on the organisation website which shows the exam results of children eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a RISE Trust laptop containing non-encrypted personal data about children

17. Training

All staff and trustees 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 organisation's processes make it necessary.

18. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

All staff will sign that they have read and understood this policy and they agree to abide by its terms on an induction policy checklist and annual records.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our organisation's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the full Trustee board.

19. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Child Protection and safeguarding policy
- Confidentiality and Information Sharing policy
- IT policy
- Social Networking policy
- Core Recording policy

Appendix 1

The RISE Trust Workforce privacy notice (Employees, Volunteers and Contractors)

The RISE Trust is the data controller for the personal information you provide.

What employee, volunteer and contractor information does The RISE Trust collect?

The RISE Trust will use your personal information to manage the employment relationship. We collect and use this information in order to fulfil contractual obligations for further details of our legal bases refer to The RISE Trust Retention Policy and Schedule.
This information is collected in a variety of ways. For example, data will be collected through application forms, CVs; obtained from passports or other identity documents such as a driving licence; from forms completed when applying for a position or during employment; from correspondence; or through interviews, meetings or other assessments.

This includes:

- your name, address, date of birth and gender and contact details including your email address and telephone number.
- your application form or CV with details of your qualifications, skills, experience, employment history including volunteering.
- your terms and conditions of employment as detailed in your contract of employment.
- details of your bank account and national insurance number to administer your pay and other contractual benefits such as pension deductions, tax and national insurance contributions.
- information about your renumeration, including entitlement to benefits such as pensions, child care vouchers, etc.
- information about your marital status, next of kin, dependants and emergency contacts.
- pre-employment checks including criminal record checks, nationality and entitlement to work in the UK checks and reference checks.
- details of your work schedule (days of work and working hours), information about absences including annual leave, sickness absence, unpaid leave, family leave (maternity/paternity/adoption etc) and the reasons for the leave.
- information about medical or health conditions and if there is the need for reasonable adjustments. Correspondence and information relating to sickness absence reviews.
- details of any complaints, disciplinary or grievance procedures in which you have been involved, including any warnings issued and related correspondence.
- assessments of your performance, including appraisals, one to one supervisory meetings and any improving work performance plans and related correspondence.
- details of trade union membership.
- equal opportunities monitoring information including information about your ethnic origin, sexual orientation and religion or belief.

What is the data being used for?

The RISE Trust needs to process data to meet its obligations with you under your employment contract, to pay you and to administer benefit and pension entitlements.

In some cases, The RISE Trust needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check an employee's entitlement to work in the UK, to deduct tax, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled.

In other cases, in order to deliver its services, The RISE Trust needs to process personal employee data before, during and after the end of the employment relationship including to:

- run recruitment and promotion processes.
- maintain accurate and up-to-date employment records and contact details and records of employee contractual and statutory rights during employment and those connected to the termination and transfer of employment including TUPE.
- operate and keep records of employee relations including complaints, disciplinary, grievance and safeguarding processes to ensure acceptable conduct within the workplace.
- operate and keep a record of employee appraisal and performance and related processes to plan for career development, succession planning and workforce management purposes.
- undertake workforce, management and organisational planning activities, including completing statutory and legislative returns, to ensure effective operations of The RISE Trust.
- operate and keep a record of absence and absence management procedures to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled.
- information about medical or health conditions including occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law and ensure that employees are receiving the pay or other benefits to which they are entitled.
- operate and keep a record of all leave (including annual, maternity, paternity, adoption, parental and shared parental leave etc.) to allow effective workforce management and to ensure that The RISE Trust complies with its duties in relation to leave entitlement and that employees are receiving the pay or other benefits to which they are entitled.
- ensure effective general HR and business administration.
- provide references on request for current or former employees.
- respond to and defend against any legal claims.

The lawful bases on which we process this information:

- Contractual bases in order to process your personal data
- Legitimate interests to use your data in ways you would reasonably expect, and which have a minimal privacy impact, or where there is a compelling justification for the processing

- Special categories to process other special categories of personal data, such as information about ethnic origin, sexual orientation or religion or belief, this is done for the purposes of equal opportunities monitoring. This is to carry out the Trust's obligations and exercise specific rights in relation to employment

Who will the data be obtained from?

In some cases, The RISE Trust may collect personal data about you from third parties, such as references supplied by former employers, information from employment background check providers, information from credit reference agencies and information from criminal records checks permitted by law.

Who will your data be shared with?

The RISE Trust will only share your data with third parties where it is required to do so and permitted under legislation e.g. in order to obtain pre-employment references, obtain employment checks from third-party providers and obtain necessary criminal records checks from the Disclosure and Barring Service (DBS). For applicants who require permission to work in the United Kingdom The RISE Trust may need to share personal data with legal advisers and the Home Office to make sure it complies with immigration requirements.

The RISE Trust will also share data with third parties that process data on its behalf e.g. in connection with payroll, the provision of benefits and the provision of occupational health services, Wiltshire Local Authority, Monahans (auditors), UCheck (DBS), HMRC, relevant pension funds and the Ministry of Justice.

Who has access to data?

The RISE Trust will share your personal data within The Trust internally where necessary including your line manager, managers in the service area in which you work and managers if you are transferring to another service area.

How does the organisation protect data?

The RISE Trust takes the security of your data seriously. The RISE Trust has internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed and is not accessed except by its employees in the performance of their duties.

Where The RISE Trust engages third parties to process personal data on its behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

For how long does The RISE Trust keep data?

The RISE Trust will hold your personal data for the duration of your employment and to comply with statutory legislation. The periods for which your data is held after the end of employment are detailed in The RISE Trust retention schedule.

Your rights

As a data subject you have a number of rights.

Your rights are set out in Articles 13 to 22 of the General Data Protection Regulation 2016 and include:

- the right to access your personal information, to request rectification or erasure of certain personal information and to object to processing in certain circumstances.
- the right to withdraw any consent you may have given to process your personal information.
- the right to complain to the Information Commissioner if you feel we are processing your personal information unlawfully.
- the right to restrict processing activity in certain circumstances.
- the right to object to certain types of processing activity.

If you would like to exercise any of these rights, please contact Lynn Evans, CEO.

What if you do not provide personal data?

Under your employment contract you have some obligations to provide The RISE Trust with data. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. You may also have to provide The RISE Trust with data to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights.

Certain information, such as contact details, your right to work in the UK and payment details, have to be provided to enable the organisation to enter a contract of employment with you. If you do not provide this information, this will hinder The RISE Trust's ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

Automated decision-making

Employment decisions are not based solely on automated decision-making.

Changes to the information

- We regularly review and, where necessary, update our privacy information and publish this on our website www.therisetrust.org
- If we plan to use personal data for a new purpose, we update our privacy information and communicate the changes to individuals before starting any new processing.

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concerns in the first instance. Alternatively, you can contact the information Commissioners office at https://ico.org.uk/concerns/

Our DPO company is One-West and is contactable via www.onewest.co.uk 01225 477944

The RISE Trust privacy notice
(Children, young people and families)

The RISE Trust is the data controller for the personal information you provide.

The categories of information that we collect, process, hold and share include:

- Personal information (such as name, address, phone number)
- Characteristics (such as ethnicity, language, disability, 2-year and 3-year funding eligibility)
- Relevant medical information
- Special educational needs information
- Assessment information
- Behavioural information
- Attendance information inc number of absences and absence reasons
- Social care involvement inc Children in Need, Child Protection or Looked After
- Anti-social behaviour (such as involvements with police, courts, probation and violence in the home)
- Aspects relating to your employment

Why we collect and use this information:

We use children's, young person's and family data to:

- Enable us to carry out specific functions and statutory returns for which we are responsible
- Produce statistics which inform decisions eg funding services
- Assess performance and set targets for educational purposes
- Support children, young people and families and monitor their progress
- Provide appropriate support and pastoral care
- Promote welfare, safeguarding, health and well-being for children, young people and families
- Assess and evaluate how well The RISE Trust services are doing as a whole and report that to the Local Authority
- We do not do any profiling on personal data
- No data is transferred out of the EU

The lawful bases on which we process this information:

- Legitimate interests - to use your data in ways you would reasonably expect, and which have a minimal privacy impact, or where there is a compelling justification for the processing
- Public tasks – in order to carry out tasks in the public interest/ safeguarding
- Special categories - to process other special categories of personal data, such as information about ethnic origin, sexual orientation or religion or belief, this is done for the purposes of equal opportunities monitoring. This is to carry out the Trust's obligations and exercise specific rights in relation to employment

We collect and use this information under:

- Care Act 2014
- Child care Act 2006
- Children Act 1989 and 2004
- Children and Families Act 2014
- Children and Social Work Act 2017
- Crime and disorder Act 1998
- Data protection Act 1998
- Education Act 1996 and 2002
- Education (SEN) regulations 2001
- Education (Information about Children in Alternative provision) (England) Regulations 2007
- Education (Information about Individual Pupil) (England) Regulations 2013
- Educations and Skills Act 2008
- The Health and Social Act 2012
- Health and Social care (Safety and Quality) Act 2015
- Immigration and Asylum Act 1999
- Learning and Skills Act 2000
- Local Government Act 2000
- Protection of Freedoms Act 2012
- Protection of Young Children Act 1999
- Young People's Act 2008

Collecting this information

Whilst some of the children and young person's information you provide us is compulsory, some of it is provided to us on a voluntary basis. We will inform you whether you are required to provide certain information to us or if you have a choice in this.

Storing the information

We hold children, young person's and family's data where necessary and fair to do so. The information is held securely by The RISE Trust as both manual and electronic files, and we will securely delete any personal data when no longer required in accordance with our published retention schedule (available on request).

Who we share this information with

We routinely share children, young person's and family information with:

- The Department for Education (DfE)
- Wiltshire Local Authority
- Public agencies - such as the NHS and health organisations, Department of Work and Pensions, the Police, probation services, schools and pre-school settings, other local authorities, the Youth Offending Team, social care.

This is to help the government and local service providers to provide support to children, young person's and families, evaluate effectiveness, improve services over time and to help improve the service families receive.

Why we share this information

We share children and young person's data with the DFE on a statutory basis under section 3 of the Education (information about individual pupils) (England) Regulations 2013. This data sharing underpins Children's Centre funding, educational attainment and monitoring (in Early Years settings). This enables them to produce the statistics and assess performance.
We also share information to promote the welfare, health and well-being of children and young people to fulfil our obligations under Section 507B of the Education Act 1996. We do not share information about children, young people and families without consent unless the law and our policies allow us to do so or there are safeguarding concerns.

Child protection information sharing

If your child is subject to child protection action plan or is a child in care, we may be part of the multi-agency group that supports them. In such cases we will record data given to us under the relevant acts.

School/early years settings

All schools and Early Years settings, as data controllers, should have privacy notices in place - they should be available on their websites.

Requesting access to personal data

Parents, young person's and children have the right to request access to information about them that we hold. To make a request for a personal information, or be given access to your child's education record, please write to The RISE CEO, Lynn Evans, to make a request. Please be as specific as you can about the information you seek as this helps us to find it as quickly as possible.
You also have the right to:

- object to processing of personal data that is likely to cause or is causing damage or distress
- Prevent processing for the purpose of direct marketing
- Object to decisions being taken by automated means
- In certain circumstances having accurate personal data rectified blocked and raised or destroyed
- Claim compensation for damages caused by breach of the data protection regulations

Changes to the information

- We regularly review and, where necessary, update our privacy information and publish this on our website www.therisetrust.org
- If we plan to use personal data for a new purpose, we update our privacy information and communicate the changes to individuals before starting any new processing.

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concerns in the first instance. Alternatively, you can contact the information Commissioners office at https://ico.org.uk/concerns/

Our DPO company is One-West and is contactable via www.onewest.co.uk 01225 477944

The RISE Trust Workforce privacy notice
Cookie Policy

About this cookie policy

This Cookie Policy explains what cookies are and how we use them. You should read this policy to understand what cookies are, how we use them, the types of cookies we use i.e, the information we collect using cookies and how that information is used and how to control the cookie preferences. For further information on how we use, store and keep your personal data secure, see our Privacy Policy.
You can at any time change or withdraw your consent from the Cookie Declaration on our website.
Learn more about who we are, how you can contact us and how we process personal data in our Privacy Policy.
Your consent applies to the following domains: www.therisetrust.org
Your current state:No consent given. Manage your consent.

What are cookies ?

Cookies are small text files that are used to store small pieces of information. The cookies are stored on your device when the website is loaded on your browser. These cookies help us make the website function properly, make the website more secure, provide better user experience, and understand how the website performs and to analyse what works and where it needs improvement.

How do we use cookies ?

As most of the online services, our website uses cookies first-party and third-party cookies for a number of purposes. The first-party cookies are mostly necessary for the website to function the right way, and they do not collect any of your personally identifiable data.
The third-party cookies used on our websites are used mainly for understanding how the website performs, how you interact with our website, keeping our services secure, providing advertisements that are relevant to you, and all in all providing you with a better and improved user experience and help speed up your future interactions with our website.

What types of cookies do we use ?

Essential: Some cookies are essential for you to be able to experience the full functionality of our site. They allow us to maintain user sessions and prevent any security threats. They do not collect or store any personal information. For example, these cookies allow you to log-in to your account and add products to your basket and checkout securely.

Statistics: These cookies store information like the number of visitors to the website, the number of unique visitors, which pages of the website have been visited, the source of the visit etc. These data help us understand and analyse how well the website performs and where it needs improvement.

Marketing: Our website displays advertisements. These cookies are used to personalize the advertisements that we show to you so that they are meaningful to you. These cookies also help us keep track of the efficiency of these ad campaigns.

The information stored in these cookies may also be used by the third-party ad providers to show you ads on other websites on the browser as well.
Functional: These are the cookies that help certain non-essential functionalities on our website. These functionalities include embedding content like videos or sharing contents on the website on social media platforms.

Preferences: These cookies help us store your settings and browsing preferences like language preferences so that you have a better and efficient experience on future visits to the website.

How can I control the cookie preferences?

Should you decide to change your preferences later through your browsing session, you can click on the "Privacy & Cookie Policy" tab on your screen. This will display the consent notice again enabling you to change your preferences or withdraw your consent entirely.
In addition to this, different browsers provide different methods to block and delete cookies used by websites. You can change the settings of your browser to block/delete the cookies. To find out more out more on how to manage and delete cookies, visit wikipedia.org, www.allaboutcookies.org.

Our DPO company is One-West and is contactable via www.onewest.co.uk 01225 477944

The RISE Trust Right to Access flowchart

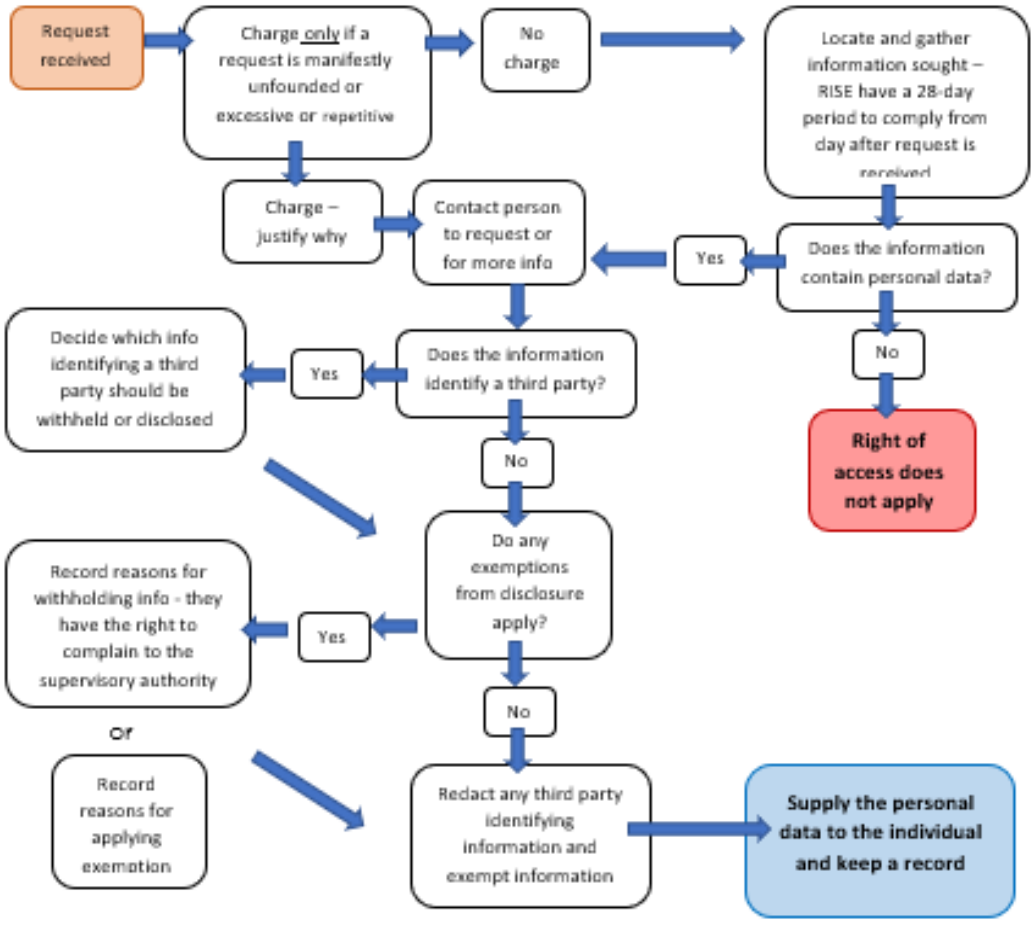
The GDPR applies to the processing of personal data that is:

- wholly or partly by automated means; or
- other processing of personal data which forms part of a filing system.

Personal data only includes information relating to natural persons who:

- can be identified or who are identifiable, directly from the information in question; or
- who can be indirectly identified from that information in combination with other information.
- Personal data may also include special categories of personal data or criminal conviction and offences data.
- Pseudonymised data can help reduce privacy risks by making it more difficult to identify individuals, but it is still personal data.
- Information about individuals acting as sole traders, employees, partners and company directors where they are individually identifiable, and the information relates to them as an individual may constitute personal data.

Please see The RISE Trust Privacy policy explaining why we keep personal data



The RISE Trust may ask the individual to provide 2 forms of identification and may contact the individual via phone to confirm the request was made. The RISE Trust will only extend the time to respond by a further two months if the request is complex or there have been a number of requests from the individual. The RISE must let the individual know within one month of receiving their request and explain why the extension is necessary.

Further guidance can be found at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

Appendix 4

Appendix 5

[Your full address]

[Phone number]

[The date]

[Name and address of the organisation]

Dear Sir or Madam

Subject access request

[Your full name and address and any other details to help identify you and the information you want.]

Please supply the information about me I am entitled to under the Data Protection Act 1998 relating to: [give specific details of the information you want, for example

- your personnel file;
- emails between 'A' and 'B' (between 1/6/17 and 1/9/17);
- your medical records (between 2016 & 2018)

If you need any more information from me please let me know as soon as possible.

It may be helpful for you to know that a request for information under the General Data Protection Act 2018 should be responded to within 28 days.

If you do not normally deal with these requests, please pass this letter to your Data Protection Officer. If you need advice on dealing with this request, the Information Commissioner's Office can assist you and can be contacted on 0303 123 1113 or at ico.org.uk

Yours faithfully

[Signature]

Record retention policy

1 Introduction

1.1 This policy sets out how long employment-related information will normally be held by us and when that information will be confidentially destroyed.

2 Responsibility

2.1 Data protection officer or Chief Executive Officer is responsible for implementing and monitoring compliance with this policy.

2.2 They will undertake an annual review of this policy to verify that it is in effective operation.

3 Our process

3.1 Information (hard copy and electronic) will be retained for at least the period specified in our Records retention schedule (sometimes known as a Data retention schedule or guidelines) (see The RISE Trust Data retention schedule).

3.2 All information must be reviewed before destruction to determine whether there are special factors that mean destruction should be delayed, such as potential litigation, complaints or grievances.

3.3 Hard copy and electronically-held documents and information must be deleted at the end of the retention period.

3.4 Hard copy documents and information must be disposed of by shredding.

Appendix 7

The RISE Trust Clean Desk Policy

July 2018

Overview

To improve the security and confidentiality of information, the RISE Trust has adopted a Clean Desk Policy for computer and workstation use.

This ensures that all sensitive and confidential information, whether on paper, storage device or a hardware device, is properly locked away and disposed of when the workstation is not in use. This policy will reduce the risk of unauthorised access, loss of or damage to information during and outside of normal business hours when workstations are left unattended.

The Clean Desk policy is an important security and privacy control and necessary for GDPR compliance.

Scope

This policy applies to all permanent, temporary and contracted staff working at any RISE Trust Centre.

Policy

Whenever a desk is left unattended for an extended period of time, the following will apply:

1) All sensitive and confidential paperwork must be removed from the desk and locked away. This includes any storage devices such as DVD, CD and USB drives.
2) All waste paperwork which contains sensitive or confidential information must be shredded. Every-one is responsible for ensuring their own confidential waste is shredded at the end of each day. **Under no circumstances should this information be placed in the normal waste.**
3) Computer workstations must be locked when the desk is unoccupied and completely shut down at the end of the working day.
4) Laptops, tablets and other hardware devices must be removed from the desk and locked in a drawer or filing cabinet.
5) Keys for accessing drawers and filing cabinets should not be left unattended at a desk.
6) Printers should be treated with the same care under this policy:
   - Any print jobs containing sensitive and confidential paperwork should be retrieved immediately. When possible the "locked print" functionality should be used.
   - All paperwork left over at the end of the work day will be properly disposed of by shredding or locked away.

The RISE Trust Data Breach flowchart

Identify breach
This may include, for example, the loss of a USB stick, **data** being destroyed or sent to the wrong address, the theft of a laptop or hacking. wrong address, the theft of a laptop or hacking.

Report to data controller
what has happened; when and how you found out about the breach; the people that have been or may be affected by the breach

RISE impact assessment
The RISE is required by law to notify the affected individuals, if a data breach is likely to result in a high risk to their rights and freedoms and notification.

Report to DPO if required (OneWest 01225 477944)

- what has happened;
- when and how The RISE found out about the breach;
- the people that have been or may be affected by the breach;
- what The RISE is doing as a result of the breach;
- who else the RISE has told

DPO to report to ICO
The RISE DPO will make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals

To report a **breach**, call ICO helpline 0303 123 1113
Normal opening hours are Monday to Friday between 9am and 4.30pm.

- what has happened;
- when and how The RISE found out about the breach;
- the people that have been or may be affected by the breach;
- what The RISE is doing as a result of the breach;
- who the ICO should contact if we need more information and who else The RISE has told.

Further guidance can be found at: https://ico.org.uk/for-organisations/report-a-breach/

Date: XX/XX/XXXX

Between:

The RISE Trust

and

Organisation Name and Address (the "Processor").

This Agreement is to ensure there is in place proper arrangements relating to personal data passed from The RISE Trust to the Processor.

This Agreement is compliant with the requirements of the General Data Protection Regulation.

Both parties wish to record their commitments under this Agreement.

Both Parties Agree:

1. Definitions

"Data" means personal data passed under this Agreement, particularly [*describe personal data being passed*];

"Services" refers to [*describe the services provided*].

2. Data Processing

The RISE Trust is the data controller for the Data and the Processor is the data processor. The Processor agrees to process the Data in accordance with Data Protection Laws and in particular on the following conditions:

a) The Processor shall only process the Data (i) on the written instructions from The RISE Trust (ii) only process the Data for completing the Services and (iii) only process the Data in the UK with no transfer of the Data outside of the UK

b) Ensure that all employees and other representatives accessing the Data are (i) aware of the terms of this Agreement and (ii) have received comprehensive training on Data Protection Laws and related good practice, and (iii) are bound by a commitment of confidentiality

c) The RISE Trust and the Processor have agreed to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, complying with Article 32 of GDPR, details of those measures are set out under Part A of the Annex to this Agreement

d) The Processor shall not involve any third party in the processing of the Data without the consent of The RISE Trust. Such consent may be withheld without reason. If consent is given a further processing agreement will be required.

e) Taking into account the nature of the processing, assist The RISE Trust by appropriate technical and organisational measures, in so far as this is possible, for the fulfilment of The RISE Trust's obligation to respond to requests from individuals exercising their rights laid down in Chapter III of GDPR – rights to

erasure, rectification, access, restriction, portability, object and right not to be subject to automated decision making etc

f) Assist The RISE Trust in ensuring compliance with the obligations pursuant to Articles 32 to 36 of GDPR – security, notification of data breaches, communication of data breaches to individuals, data protection impact assessments and when necessary consultation with the ICO etc, taking into account the nature of processing and the information available to the Processor.

g) At The RISE Trust's choice safely delete or return the Data at any time. [It has been agreed that the Processor will in any event securely delete the Data at the end of the Services]. Where the Processor is to delete the Data, deletion shall include destruction of all existing copies unless otherwise a legal requirement to retain the Data. Where there is a legal requirement the Processor will prior to entering into this Agreement confirm such an obligation in writing to The RISE Trust. Upon request by The RISE Trust the Processor shall provide certification of destruction of all Data.

h) Make immediately available to The RISE Trust all information necessary to demonstrate compliance with the obligations laid down under this Agreement and allow for and contribute to any audits, inspections or other verification exercises required by The RISE Trust from time to time.

i) Maintain the integrity of the Data, without alteration, ensuring that the Data can be separated from any other information created; and

j) Immediately contact The RISE Trust if there is any personal data breach or incident where the Data may have been compromised.

For and on behalf of **The RISE Trust**

……

For and on behalf of [XXXXXXX]

……