Data Protection Policy

RIDGEWAY EDUCATION TRUST

Approved by Trust Board: 12 May 2020

Review date: May 2022

Contents

1. Policy statement

Ridgeway Education Trust (RET) aims to ensure that all personal data collected about staff, pupils, parents, members, directors, governors, 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.

Any breach of this policy will be taken seriously and may result in disciplinary action.

2. About this policy

The types of information that we may be required to handle include:

- school admission and attendance registers;
- students' curricular records;
- reports to parents/guardians on the achievements of their children;
- records in connection with students entered for prescribed public examinations;
- staff records, including payroll records;
- student disciplinary records;
- personal information for teaching purposes;
- records of contractors and suppliers.

This policy has been approved by the RET Trust Board. It sets out RET's rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

This policy does not form part of any employee's contract of employment and may be amended at any time.

RET is responsible for ensuring compliance with the Act and with this policy. If you consider that the policy has not been followed in respect of personal data about yourself or others you should raise the matter with your line manager or make a complaint to RET using RET's Complaints Procedure.

3. 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 meets the requirements of the Protection of Freedoms Act 2012 when referring to RET's use of biometric data.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with RET's funding agreement and articles of association.

4. 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.

5. The data controller

RET processes personal data relating to parents, pupils, staff, members, directors, governors, visitors and others, and therefore is a data controller.

RET is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

6. Roles and responsibilities

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

6.1 Trust Board

The Trust Board has overall responsibility for ensuring that RET and all RET schools comply with all relevant data protection obligations.

6.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring RET's compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the Trust Board and, where relevant, report to the board their advice and recommendations on RET data protection issues.

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

The DPO role is externally contracted through Turn IT On. The DPO can be contacted through the Trust Director of Finance & Services or directly via dpo@@turniton.co.uk

6.3 Executive Headteacher

The Executive Headteacher acts as the most senior representative of the data controller with control on a day-to-day basis overseen by each school Headteacher, the Director of Didcot Sixth Form and the Director of Finance & Services.

6.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing RET 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

The Director of Finance & Services will act as an internal Trust contact point for the Data Protection Officer when looking for advice and guidance.

7. Data protection principles

The GDPR is based on data protection principles that RET and all RET schools must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how RET aims to comply with these principles.

8. Collecting personal data

8.1 Lawfulness, fairness and transparency

RET will only process personal data where there are one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that RET can **fulfil a contract** with the individual, or the individual has asked RET to take specific steps before entering into a contract

- The data needs to be processed so that RET 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 RET, 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 RET 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, RET will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

Where online services to pupils, such as classroom apps, are offered and RET intends to rely on consent as a basis for processing, parental consent will be obtained where the pupil is under 13 (except for online counselling and preventive services).

Whenever RET first collects personal data directly from individuals, they will be provided with the relevant information required by data protection law.

8.2 Limitation, minimisation and accuracy

RET will only collect personal data for specified, explicit and legitimate reasons. RET will explain these reasons to the individuals when RET first collects their data.

If personal data is to be used for reasons other than those given when it was first obtained, RET will inform the individuals concerned before doing so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with RET's Records Management Policy.

9. Sharing personal data

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

- There is an issue with a pupil or parent/carer that puts the safety of RET staff at risk
- There is a need to liaise with other agencies – RET will seek consent as necessary before doing this
- RET's suppliers or contractors need data to enable services to be provided to staff and pupils – for example, IT companies. When doing this, RET 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 that is shared
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with RET

RET will also share personal data with law enforcement and government bodies where it is 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 RET safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

RET may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any RET pupils or staff.

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

10. Subject access requests and other rights of individuals

10.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that RET 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. 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 via the Director of Finance & Services.

10.2 Children and subject access requests

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

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils aged 12 and above 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.

10.3 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 RET will comply within 3 months of receipt of the request, where a request is complex or numerous. RET will inform the individual of this within 1 month, and explain why the extension is necessary

RET will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil 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, RET 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 RET refuses a request, RET will tell the individual why, and tell them they have the right to complain to the ICO.

10.4 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 RET is collecting their data about how RET uses and processes 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

Consideration will be given to requests from parents, or those with parental responsibility, to access their child's educational record on a case-by-case basis.

12. Biometric recognition systems

Where RET uses pupils' biometric data as part of an automated biometric recognition system, RET will comply with the requirements of the Protection of Freedoms Act 2012.

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

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

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

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, RET will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use RET's biometric system(s), RET will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and RET will delete any relevant data already captured.

13. CCTV

RET uses CCTV in various locations around RET sites to ensure it remains safe. RET will adhere to the ICO's code of practice for the use of CCTV.

RET does not need to ask individuals' permission to use CCTV, but RET makes it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to Catherine Steele, RET Operational Services Lead.

14. Photographs and videos

As part of school activities, RET may take photographs and record images of individuals within RET schools.

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

Where RET needs parental consent, RET will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where RET don't need parental consent, RET will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- Within RET schools on notice boards and in RET school magazines, brochures, newsletters, etc.
- Outside of RET schools by external agencies such as photographers, newspapers, campaigns
- Online on RET school websites or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, RET will delete the photograph or video and not distribute it further.

When using photographs and videos in this way RET will not accompany them with any other personal information about the child, to ensure they cannot be identified.

See Use of Photos and Videos Policy for more information.

15. Data protection by design and default

RET will put measures in place to show that RET has integrated data protection into all of its data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where RET'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; RET will also keep a record of attendance
- Regularly conducting reviews and audits to test RET privacy measures and make sure RET is compliant
- Maintaining records of RET processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of RET academies and DPO and all information RET is required to share about how RET uses and processes their personal data (via privacy notices)
    - For all personal data that RET holds, maintaining an internal record of the type of data, data subject, how and why RET is using the data, any third-party recipients, how and why RET is storing the data, retention periods and how RET is keeping the data secure

16. Data security and storage of records

RET will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the relevant RET school admin office, e.g. relating to trips and visits
- Passwords that are at least 8 characters long containing letters and numbers are used to access RET computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Where staff or students need access to sensitive personal information on remote devices, they are expected to do so from OneDrive or a GDPR-compliant cloud-based server
- If sensitive personal data is stored on portable devices such as laptops and USB drives, encryption will be used. Encrypted devices are only issued after agreement by the Headteacher
- Where RET needs to share personal data with a third party, RET will carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

17. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where RET cannot or do not need to rectify or update it.

For example, RET will shred paper-based records, and overwrite or delete electronic files. Where RET uses a third party to safely dispose of records on its behalf, the third party will be required to provide sufficient guarantees that it complies with data protection law.

18. Personal data breaches

RET will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, RET will follow the procedure set out in appendix 1.

When judged appropriate, the RET DPO will report the data breach to the ICO within 72 hours. Such breaches may include, but are not limited to:

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

19. Training

All staff 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 RET's or one of RET's academies' processes make it necessary.

20. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed by the Trust Board **every 2 years**.

21. Links to other policies/procedures

i. CCTV Policy for RET Secondary Schools

ii. Use of Images (Photographs) and Videos Procedure

iii. Privacy Notice for pupils

iv. Privacy Notice for staff

v. Privacy Notice for RET Trustees and Governors

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO and the PA to the Headteacher of each relevant secondary school, or the School Business Partner in respect of our primary school(s), who will keep a register of notifications.
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will alert the Executive Headteacher, Headteacher and Company Secretary, who will advise the Trust Director identified as its lead on data protection.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are notified by the DPO to the Company Secretary, who will store records within a designated file within the RET network.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO

expects to have further information. The DPO will submit the remaining information as soon as possible

- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches are notified by the DPO to the Company Secretary, who will store records within a designated file within the RET network.
- The DPO and an officer designated by the Executive Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

RET will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. RET will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- *If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error*
- *Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error*
- *If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it*
- *In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way*
- *The DPO will ensure RET receives a written response from all the individuals who received the data, confirming that they have complied with this request*
- *The DPO will carry out an internet search to check that the information has not been made public; if it has, RET will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted*