REDHILL ACADEMY TRUST

DATA PROTECTION POLICY

APPROVING BODY	Trust Executive Board
DATE APPROVED	29/09/2021
VERSION	2.0
SUPERSEDES VERSION	1.0
REVIEW DATE	01/09/2024
LEGISLATION	Data Protection Act 2018
FURTHER INFORMATION/ GUIDANCE	UK General Data Protection Regulation (UK GDPR)

CONTENTS

STATEMENT OF INTENT

The Redhill Academy Trust (the "Trust") is required to keep and process certain information about its staff members and students/pupils in accordance with its legal obligations under the UK General Data Protection Regulation (UK GDPR).

The Trust may, from time to time, be required to share personal information about staff or students/pupils with other organisations, mainly the DfE, Local Authorities, other academies and educational bodies, and children's services departments.

This policy is in place to ensure the whole workforce, including governors are aware of their responsibilities and outlines how our academies comply with the following core principles of the UK GDPR.

Organisational methods for keeping data secure are imperative, and the Trust believes that it is good practice to keep clear practical policies, backed up by written procedures.

1. LEGAL FRAMEWORK

1.1. This policy has due regard to legislation, including, but not limited to the following:

- The UK General Data Protection Regulation (UK GDPR)
- The Education (Independent School Standards) Regulations 2014 The School Standards and Framework Act 1998

1.2. This policy will also have regard to the following guidance: Information Commissioner's Office 'Overview of the General Data Protection Regulation (GDPR)' as amended March 2021

- Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'
- Information Commissioner's Office 'Data Sharing Code of Practice (2020)'
- Information Commissioner's Office 'Data Sharing and reuse of data by competent authorities for nonlaw enforcement purposes'

1.3. This policy will be implemented in conjunction with the following other Trust policies:

- Academy E-Safety Policies
- Freedom of Information Policy
- UK GDPR Data Retention Policy
- Acceptable Use Statement for Data
- Various Privacy Notices

2. APPLICABLE DATA

2.1. For the purpose of this policy, personal data refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g. an IP address. The UK GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

2.2. A sub-set of personal data is known as 'special category personal data'. This special category data is information that relates to:

2.2.1. race or ethnic origin;

2.2.2. political opinions;

2.2.3. religious or philosophical beliefs;

2.2.4. trade union membership;

2.2.5. physical or mental health;

2.2.6. an individual's sex life or sexual orientation;

2.2.7. genetic or biometric data for the purpose of uniquely identifying a natural person.

2.3. Special category personal data is given additional protection under the UK GDPR, and further safeguards apply where this information is to be collected and used.

The UK GDPR also gives additional protection to personal data relating to criminal convictions and offences or related security measures (including information about criminal activity, allegations or suspicions, investigations and proceedings) ("criminal offence data").

3. PRINCIPLES

3.1. In accordance with the requirements outlined in the UK GDPR, the Trust and its staff must comply with the data protection principles set out in Article 5 of the UK GDPR. specifically, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

In addition, the Trust is also responsible for, and be must be able to demonstrate compliance with the above principles ('accountability'). Further details about the way in which the Trust meets its accountability obligations are set out in section 4 below.

4. ACCOUNTABILITY

4.1. The Trust will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the UK GDPR.

4.2. The Trust will provide comprehensive, clear and transparent privacy notices.

4.3. Additional internal records of processing activities will be maintained and kept up-to-date.

4.4. Internal records of processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

4.5. The Trust will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Data minimisation.
- Pseudonymisation.
- Transparency.
- Allowing individuals to monitor processing.
- Continuously creating and improving security features.

4.6. Data protection impact assessments will be used, where appropriate.

5. DATA PROTECTION OFFICER (DPO)

5.1. A DPO has been appointed in order to:

- Inform and advise the Trust and its staff about their obligations to comply with the UK GDPR and other data protection laws.
- Monitor the Trust's compliance with UK GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments (where appropriate), conducting internal audits, and providing the required training to staff members.

5.2. The Director of Operations is appointed as DPO and has professional experience and knowledge of data protection law, particularly that in relation to education. The DPO is contactable at DPO@redhillacademytrust.org.uk.

5.3. The DPO will work on day to day duties for compliance on UK GDPR alongside individual academy Operations Managers, who are appointed as Data Protection Leads for their academy.

5.4. The DPO reports to the highest level of management at the Trust, which is the Trust Principal.

5.5. The DPO will report termly on data protection compliance to the Audit and Risk Committee of the Executive Board.

5.6. The DPO will operate independently and will not be dismissed or penalised for performing their task.

5.7. Sufficient resources will be provided to the DPO to enable them to meet their obligations.

6. LAWFUL PROCESSING

6.1. The Trust is responsible for ensuring that personal data is processed in a lawful, fair and transparent way.

6.2. The legal basis for processing data will be identified and documented in relation to any processing activity the Trust carries out, before the processing begins, and then regularly while it continues.

6.3. Under Article 6 UK GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained.
- Processing is necessary for:
  - — Compliance with a legal obligation.
  - — The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
  - — For the performance of a contract with the data subject or to take steps to enter into a contract.
  - — Protecting the vital interests of a data subject or another person.
  - — For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (This condition is not available to processing undertaken by the individual academy in the performance of its tasks.)

Where special category personal data or criminal offence data is processed, the Trust will also identify a lawful condition (as set out in Articles 9 and 10 of the UK GDPR, and Schedule 1 of the DPA 2018) for processing this type of information, and document it."

7. CONSENT

7.1. Consent will be sought prior to processing any data which cannot be done so under any other lawful basis, such as complying with a regulatory requirement.

7.2. Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

7.3. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

7.4. Where consent is given, a record will be kept documenting how and when consent was given.

7.5. The Trust will ensure that consent mechanisms meet the standards of the UK GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

7.6. Consent accepted under the DPA (2018) will be remain in place until it is withdrawn by the data subject.

7.7. Consent can be withdrawn by the individual at any time.

7.8. When gaining student/pupil consent, consideration will be given to the age, maturity and mental capacity of the student/pupil in question. Consent will only be gained from students/pupils where it is deemed that the student/pupil has a sound understanding of what they are consenting to.

8. THE RIGHT TO BE INFORMED

8.1. The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

8.2. If services are offered directly to a child, the individual academy will ensure that the privacy notice is written in a clear, plain manner that the child will understand.

8.3. Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided.

8.4. Where data is not obtained directly from the data subject, information regarding the categories of personal data that the individual academies hold, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.

8.5. For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

8.6. In relation to data that is not obtained directly from the data subject, this information will be supplied:

- Within one month of having obtained the data.
- If disclosure to another recipient is envisaged, at the latest, before the data is disclosed.

  If the data is used to communicate with the individual, at the latest, when the first communication takes place.

9. THE RIGHT OF ACCESS

9.1. Anybody has the right to ask the Trust to see a copy of any personal data held about them together with other information about how their information is used (known as supplementary information). This legal right is called the right of subject access. When someone exercises this legal right, they will be making a Subject Access Request or SAR.

9.2. Where necessary, the Trust will verify the identity of the person making the request before any information is supplied.

9.3. A copy of the information will be supplied to the individual free of charge; however, the individual academy may impose a ‘reasonable fee’ to comply with requests for further copies of the same information.

9.4. Where possible, the information will be provided in a commonly used electronic format.

9.5. Where a request is excessive, a reasonable fee will be charged.

9.6. All fees will be based on the administrative cost of providing the information.

9.7. All requests will be responded to without delay and at the latest, within one month of receipt (subject to the below).

9.8. In the event of numerous or complex requests, the Trust has the right to extend the time limit for a response by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

9.9. Where a request is manifestly unfounded, excessive or repetitive, the Trust holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy.

10. THE RIGHT TO RECTIFICATION

10.1. Individuals are entitled to have any inaccurate or incomplete personal data rectified in certain circumstances.

10.2. Where the personal data in question has been disclosed to third parties, the academy will inform them of the rectification where possible.

10.3. Where appropriate, the Trust will inform the individual about the third parties that their personal data has been disclosed to.

10.4. Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

10.5. Where no action is being taken in response to a request for rectification, the academy will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

10.6. Any request for rectification should be sent to the Academy Data Protection Lead without undue delay. The request must be complied with within one calendar month (unless this deadline is extended in accordance with the UK GDPR).

11. THE RIGHT TO ERASURE

11.1. Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

11.2. Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

11.3. The academy has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information.
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- For public health purposes in the public interest.
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes.
- The exercise or defence of legal claims.

11.4. As a student/pupil may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a student/pupil has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

11.5. Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

11.6. Where personal data has been made public within an online environment, the Trust will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

11.7. Any request for erasure should be sent to the Academy Data Protection Lead without undue delay. The request must be complied with within one calendar month (unless this deadline is extended in accordance with the UK GDPR).

12. THE RIGHT TO RESTRICT PROCESSING

12.1. Individuals have the right to block or suppress the Trust's processing of personal data.

12.2. In the event that processing is restricted, the Trust will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

12.3. The Trust will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the academy has verified the accuracy of the data.
- Where an individual has objected to the processing and the academy is considering whether their legitimate grounds override those of the individual.
- Where processing is unlawful and the individual opposes erasure and requests restriction instead.
- Where the academy no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.

12.4. If the personal data in question has been disclosed to third parties, the Trust will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

12.5. The Trust will inform individuals when a restriction on processing has been lifted.

12.6. Any request for erasure should be sent to the Academy Data Protection Lead without undue delay. The request must be complied with within one calendar month (unless this deadline is extended in accordance with the UK GDPR).

13. THE RIGHT TO DATA PORTABILITY

13.1. Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

13.2. Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

13.3. The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller.
- Where the processing is based on the individual's consent or for the performance of a contract.
- When processing is carried out by automated means.

13.4. Personal data will be provided in a structured, commonly used and machine-readable form.

13.5. The Trust will provide the information free of charge.

13.6. Where feasible, data will be transmitted directly to another organisation at the request of the individual.

13.7. The Trust is not required to adopt or maintain processing systems which are technically compatible with other organisations.

13.8. In the event that the personal data concerns more than one individual, the academy will consider whether providing the information would prejudice the rights of any other individual.

13.9. Any request for data portability should be sent to the Data Protection Lead without undue delay. The request must be complied with within one calendar month (unless this deadline is extended in accordance with the UK GDPR).

Where no action is being taken in response to a request, the academy will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

14. THE RIGHT TO OBJECT

14.1. The Trust will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

14.2. Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest.
- Direct marketing.
- Processing for purposes of scientific or historical research and statistics.

14.3. Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.
- The academy will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the academy can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

14.4. Where personal data is processed for direct marketing purposes:

- The Trust will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The Trust cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

14.5. Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the Trust is not required to comply with an objection to the processing of the data.

1.6. Any objection should be sent to the Academy Data Protection Lead without undue delay. The request must be complied with within one calendar month (unless this deadline is extended in accordance with the UK GDPR).

15. PRIVACY BY DESIGN AND PRIVACY IMPACT ASSESSMENTS

15.1. The Trust will act in accordance with UK GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the academy has considered and integrated data protection into processing activities.

15.2. Data protection impact assessments (DPIAs) may be used to identify the most effective method of complying with the academy's data protection obligations and meeting individuals' expectations of privacy.

15.3. DPIAs will allow the academy to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the academy's reputation which might otherwise occur.

15.4. A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

15.5. A DPIA will be used for more than one project, where necessary.

15.6. High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling.
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences.
- The use of CCTV.

15.7. The Trust will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes.
- An assessment of the necessity and proportionality of the processing in relation to the purpose.
- An outline of the risks to individuals.
- The measures implemented in order to address risk.

15.8. Where a DPIA indicates high risk data processing, the academy will consult the ICO to seek its opinion as to whether the processing operation complies with the UK GDPR.

16. DATA BREACHES

16.1. The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

16.2. The Data Protection Lead will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their data protection training.

16.3. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the Academy Data Protection Lead will inform the DPO immediately and will record details of the breach within their Data Protection File.

16.4. All notifiable breaches will be reported to the relevant supervisory authority by the DPO within 72 hours of the academy becoming aware of it.

16.5. The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.

16.6. In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the academy Data Protection Lead will notify those concerned directly.

16.7. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

16.8. In the event that a breach is sufficiently serious, the public will be notified without undue delay.

16.9. Effective and robust breach detection, investigation and internal reporting procedures are in place at the academy, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

16.10. Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned.
- The name and contact details of the DPO.
- An explanation of the likely consequences of the personal data breach.
- A description of the proposed measures to be taken to deal with the personal data breach.
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects.

16.11. Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

17. DATA SECURITY

17.1. Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

17.2. Confidential paper records will not be left unattended or in clear view anywhere with general access.

17.3. Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

17.4. Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.

17.5. Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.

17.6. All electronic devices are password-protected to protect the information on the device in case of theft.

17.7. Where possible, the academy enables electronic devices to allow the remote blocking or deletion of data in case of theft.

17.8. All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

17.9. Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.

17.10. Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

17.11. When sending confidential information by fax, staff will always check that the recipient is correct before sending.

17.12. Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the academy premises accepts full responsibility for the security of the data.

17.13. Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.

17.14. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the academy containing sensitive information are supervised at all times.

17.15. The physical security of the academy's buildings and storage systems, and access to them, is reviewed on a regular basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

17.16. The Trust takes its duties under the UK GDPR seriously and any unauthorised disclosure may result in disciplinary action.

17.17. The Academy Data Protection Leads are responsible for making sure continuity and recovery measures are in place to ensure the security of protected data.

18. PUBLICATION OF INFORMATION

18.1. The Trust and its individual academies publish on their websites information that must be made routinely available, including:

- Policies and procedures.
- Annual reports.
- Financial information.
- Governance information.

18.2. The Trust or its individual academies will not publish any personal information, including photos, on any website without the permission of the affected individual.

18.3. When uploading information to a website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

19. CCTV AND PHOTOGRAPHY

19.1. The Trust understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

19.2. The Trust notifies all students, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.

19.3. Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

19.4. CCTV footage will be kept for a period of time, as determined by individual academy CCTV Policies, and no longer than three months for security purposes; the individual academy's Data Protection Lead is responsible for keeping the records secure and allowing access.

19.5. The individual academies will always indicate their intentions for taking photographs of students/pupils and will retrieve permission before publishing them.

19.6. If the Trust wishes to use images/video footage of students/pupils in a publication, such as the academy website, prospectus, or recordings of academy plays, written permission will be sought from the parent of the student/pupil or the student/pupil themselves if 12 years or older and deemed capable of understanding the reason for processing.

19.7. Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the UK GDPR.

20. DATA RETENTION

20.1. Data will not be kept for longer than is necessary.

20.2. Unrequired data will be deleted as soon as practicable.

20.3. Some educational records relating to former students/pupils or employees of the academy may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

20.4. Paper documents will be shredded or use of a confidential waste disposal service, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

20.5. Data Retention Periods are clearly defined on the Trust Data Retention Policy.

21. DBS DATA

21.1. All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

21.2. Data provided by the DBS will never be duplicated.

21.3. Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

22. POLICY REVIEW

22.1. This policy is reviewed every three years by the DPO.