REDHILL ACADEMY TRUST

Equality and Achievement

DATA PROTECTION POLICY

APPROVING BODY	TRUST EXECUTIVE BOARD
DATE APPROVED	October 2023
VERSION	4.0
SUPERSEDES VERSION	3.0
REVIEW DATE	October 2024
FURTHER INFORMATION / GUIDANCE	Data Protection Act 2018 Equality Act 2018 UK General Data Protection Regulation (UK GDPR)

Contents

1. Statement of intent

The Redhill Academy 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 (GDPR).

An academy within the trust may, from time to time, be required to share personal information about its staff or students/pupils with other organisations, mainly the DfE, the LA, 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 Redhill Academy Trust believes that it is good practice to keep clear practical policies, backed up by written procedures.

This policy complies with the requirements set out in the GDPR, which came into effect on 25 May 2018 and updated to UK GDPR in 2020.

For the avoidance of doubt where this policy refers to the Trust, this also applies to individual Academies.

Signature (Director of Executive Board) Date

2. Legal framework

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence in education.

It also reflects the ICO's guidance 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.

In addition, this policy complies with our funding agreement and articles of association.

This policy will be implemented in conjunction with the following other academy policies:

- Online Safety Policy
- Freedom of Information Policy
- GDPR Data Retention Policy
- Data Acceptable Use Policy
- CCTV Policy
- Privacy Policies

3. Definitions

TERM	DEFINITION
Personal data	Any information relating to an identified, or identifiable, living 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.

TERM	DEFINITION
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 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.

4. The Data Controller

Our Academies process personal data relating to parents and carers, pupils, staff, governors, visitors, and others, and therefore is a data controller.

The school is registered with the ICO / has paid its data protection fee to the ICO, as legally required.

5. Principles

In accordance with the requirements outlined in the GDPR, 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 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.

The GDPR also requires that “the controller shall be responsible for, and able to demonstrate, compliance with the principles.”

6. Accountability

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

Our Academies will provide comprehensive, clear, and transparent privacy policies.

Additional internal records of each academy’s processing activities will be maintained and kept up to date.

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.

The academy 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.

Data protection impact assessments will be used, where appropriate.

7. Roles and Responsibilities

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

7.1 Governing board

The Local Academy Board has overall responsibility for ensuring that the Academy complies with all relevant data protection obligations.

7.2 Data protection officer (DPO)

A DPO has been appointed in order to:

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

The DPO will delegate day to day duties for compliance with GDPR in individual academies, to each academy Operations Manager, who are appointed as Data Controller/Lead for their academy.

The DPO reports to the Director of Operations at the Trust, who reports into the CEO.

The DPO will report annually on GDPR to the Executive Board Audit and Risk Committee.

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

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

The DPO is also the first point of contact for DPLs and for the ICO.

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

Our DPO is Linda Hayes and is contactable via DPO@redhillacademytrust.org.uk.

7.3 Headteacher

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

7.4 All staff

Staff are responsible for:

- Collecting, storing, and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the school DPL or Trust 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 UK.
  - 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

8. Collecting personal data

8.1 Lawfulness, fairness, and transparency

The legal basis for processing data will be identified and documented prior to data being processed.

Each academy will act as a data processor; however, this role may also be undertaken by other third parties.

The academy will only process personal data where we have 1 of 6 'lawful bases' (legal reasons) to do so under data protection law:

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

- The data needs to be processed to ensure the **vital interests** of the individual or another person i.e., to protect someone's life.
- The data needs to be processed so that the school, as a public authority, can **perform a task in the public interest or exercise its official authority.**
- The data needs to be processed for the **legitimate interests** of the school (where the processing is not for any tasks the school performs as a public authority) 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, the academy will also meet one of the special conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent.**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security, or social protection law.**
- The data needs to be processed to ensure the **vital interest** of the individual or another person, where the individual is physically or legally incapable of giving consent.
- The data has already been made **manifestly public** by the individual.
- The data needs to be processed for the establishment, exercise, or defense of **legal claims.**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation.
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law.
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest.

For criminal offence data, the academy will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent.**
- The data needs to be processed to ensure the **vital interest** of the individual or another person, where the individual is physically or legally incapable of giving consent.
- The data needs to be processed to ensure the **vital interest** of the individual or another person, where the individual is physically or legally incapable of giving consent.
- The data has already been made **manifestly public** by the individual.

- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise, or defense of **legal rights.**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation.

Whenever the academy first collects personal data directly from individuals, it will provide them with the relevant information required by data protection law.

The academy will always consider the fairness of our data processing. The academy will ensure the academy do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

8.2 Limitation, minimisation, and accuracy

The academy 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.

If the academy wants 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 do their jobs.

The academy will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymized. This will be done in accordance with the school's data record retention schedule.

9. Consent

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.

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

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

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

Each individual academy will ensure that consent mechanisms meet the standards of the 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.

Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be re-obtained.

Consent can be withdrawn by the individual at any time.

Where a child is under the age of 13, the consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative, or counselling services offered directly to a child.

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.

10. Sharing personal data

The academy will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk.
- The academy 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 pupils -for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors that can provide sufficient guarantees that they comply with UK data protection law.
    - Establish a contract with the supplier or contractor to ensure the fair and lawful processing of ay personal data we share.
    - Only share data that the supplier or contractor needs to carry out their service.

The academy will also share personal data with the law enforcement and government bodies where we are legally required to do so.

The academy 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 pupils or staff.

Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

11. Subject access request and other rights of individuals

11.1 Subject access requests

Individuals have a right to make a ‘subject access request’ to gain access to personal information that the school 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 is not possible, the criteria used to determine the period.
- Where relevant, the existence of the right to request rectification, erasure, or restriction, or to object to such processing.
- The right to lodge a complaint with the ICO or another supervisory authority.
- 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.
- The safeguards provided if the data is being transferred internationally.

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of the individual
- Correspondence address
- Contact number and email address.
- Details of the information requested.

If staff receive a subject access request in any form, they must immediately for to their DPL or the Trust DPO.

11.2 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 below the age of 13 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 pupils at our school 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.

11.3 Responding to a subject access request

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 (or receipt of the additional information needed to confirm identity, where relevant)
- 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.

The academy may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual.
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests.
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it.
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts?

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

11.4 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 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 (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing that has been justified on the basis of public interest, official authority or legitimate interests.
- Challenge decisions based solely on automated decision making or profiling (i.e., making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- 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 Academy DPL or Trust DPO. If staff receive such a request, they must immediately forward it to the DPL/ DPO.

11.5 The right to rectification

- Individuals are entitled to have any inaccurate or incomplete personal data rectified.

- Where the personal data in question has been disclosed to third parties, the academy will inform them of the rectification where possible.
- Where appropriate, the academy will inform the individual about the third parties that the data has been disclosed to.
- Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.
- 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.

11.6 The right to erasure

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

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.

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
- 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.

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

11.7 The right to restrict processing.

- Individuals have the right to block or suppress the academy's processing of personal data.
- In the event that processing is restricted, the academy 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.
- The academy 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.
- If the personal data in question has been disclosed to third parties, the academy will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.
- The academy will inform individuals when a restriction on processing has been lifted.

11.8 The right to data portability

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

- 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.
- 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
- Personal data will be provided in a structured, commonly used, and machine-readable form.
- The academy will provide the information free of charge.
- Where feasible, data will be transmitted directly to another organisation at the request of the individual.
- The academy is not required to adopt or maintain processing systems which are technically compatible with other organisations.
- 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.
- The academy will respond to any requests for portability within one month.
- Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.
- 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.

11.9 The right to object

- The academy 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.
- 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.

- 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.
- Where personal data is processed for direct marketing purposes:
- The academy will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The academy cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.
- 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 academy is not required to comply with an objection to the processing of the data.

12. Automated decision making and profiling.

Individuals have the right not to be subject to a decision when:

- It is based on automated processing, e.g., profiling.
- It produces a legal effect or a similarly significant effect on the individual.

The academy will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

When automatically processing personal data for profiling purposes, the academy will ensure that the appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.
- Using appropriate mathematical or statistical procedures.
- Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

Automated decisions must not concern a child or be based on the processing of sensitive data, unless:

- The academy has the explicit consent of the individual.

- The processing is necessary for reasons of substantial public interest on the basis of Union/Member State law.

13. Privacy by design and privacy impact assessments

The academy will act in accordance with the 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.

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.

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.

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.

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

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.

The academy 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.

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 GDPR.

14. Data breaches

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.

The Operations Manager will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

The DPO must be informed of all breaches as soon as possible, who will then oversee an investigation into the circumstances, focussing on containment initially in an attempt to minimise the impact of the breach. The DPO will consider whether the breach is reportable to the ICO and where necessary, will notify the ICO within 72 hours of the academy becoming aware of the breach, via the 'report a breach' page of the ICO website.

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.

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

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

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

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.

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.

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

15. Data security

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

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

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.

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.

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

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

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

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

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

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

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

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.

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.

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.

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.

Redhill Academy Trust takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

The academy Operations Manager is responsible for making sure continuity and recovery measures are in place to ensure the security of protected data.

16. Publication of information

Redhill Academy 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

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

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.

17. CCTV

The academy uses CCTV in various locations around the school site to ensure it remains safe and understands that recording images of identifiable individuals constitutes as processing personal information. The academy will follow the ICO's guidance for the use of CCTV and comply with data protection principles.

The academy needs to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Further information relating to use of CCTV can be located in the CCTV policy. Any enquiries relating to the CCTV system should be directed to the Operations Manager of the Academy.

18. Biometric recognition systems

Section not applicable for The Carlton Junior Academy.

19. Photographs and videos

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

The academy 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 the pupil.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

20. Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils, and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. The academy recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, the academy will treat this as a data breach, and will follow the personal data breach procedure.

21. Data security and storage of records

The academy 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:

- Data will not be kept for longer than is necessary.
- Unrequired data will be deleted as soon as practicable.
- 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.
- Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.
- The academy may also use a third party to safely dispose of records on the academy's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.
- 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, or left anywhere else where there is general access.
- Only essential personal information is taken off site, with the prior permission of the operations manager.
- The academy's Acceptable Use Policy must be complied with at all times when using electronic devices of any kind.
- 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 10)

22. Training

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of the continuing professional development, where changes to legislation, guidance or the academy's processes make it necessary.

23. Policy review

This policy is reviewed annually by the DPO. (The annual review frequency reflects the DfE recommendation in its advice on statutory policies).