RAVENSCLIFFE
HIGH SCHOOL & SPORTS COLLEGE

GDPR Policy/Procedures

Reviewed by	Gareth Hunter
Date approved	05/02/2026
Date for review	04/02/2027
Signed by Chair of sub committee	Simon Lea
Signed by Acting Headteacher	Jo Hague
Signed by chair of Governors (statutory policies only)	Jill Grant/Brendan Heneghan

1. Introduction

Ravenscliffe High School is committed to protecting the privacy and security of all personal data it handles. This includes information relating to staff, pupils, parents, governors, visitors, and any other individuals associated with the school.

We ensure that all personal data is collected, stored, and processed in full compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018), as amended by the Data (Use and Access) Act 2025 (DUAA). These laws govern all personal data, whether maintained in paper records or electronic systems, and set out strict requirements for lawful processing, transparency, data minimisation, accuracy, security, retention, and individual rights.

2. Legislation and Guidance

This policy reflects and complies with:

- UK GDPR and DPA 2018 (including DUAA 2025 amendments)
- ICO guidance (including CCTV and video surveillance guidance)
- The ICO's International Data Transfer Agreement (IDTA) and UK Addendum for restricted transfers;
- The Home Office Surveillance Camera Code of Practice; and
- Regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which provides parents with the right to access their child's educational record.

3. Data Controller

Ravenscliffe High School processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore acts as a data controller.

The school is registered with the Information Commissioner's Office and will renew this registration annually or as otherwise legally required.

ICO registration number: Z7471285.

4. Roles and Responsibilities

This policy applies to all staff employed by the school and to external organisations or individuals working on our behalf.

Individual/Group	Responsibility
Governing Body	Has overall responsibility for ensuring the school complies with data protection obligations.
Headteacher	Acts as the representative of the data controller on a day-to-day basis.
Data Protection Officer	Oversees implementation, monitors compliance, develops related policies/guidelines, and is the first point of contact for individuals and the ICO. **Our DPO is Debbie Pettiford (DP Advice Service).**
All Staff	Must collect, store and process personal data in accordance with this policy; promptly report suspected data breaches; seek advice from the DPO when unsure; and complete training. Failure to comply may result in disciplinary action.

5. Data Protection Principles

Under the UK GDPR, Ravenscliffe High School must adhere to the following core principles when handling personal data:

- **Lawfulness, fairness, and transparency** – Data must be processed in a lawful, fair, and transparent way.
- **Purpose limitation** – Data must only be collected for specific, explicit, and legitimate purposes and not used for anything incompatible with those purposes.
- **Data minimisation** – Information must be adequate, relevant, and limited to what is necessary for the intended purpose.
- **Accuracy** – Personal data must be accurate and kept up to date where necessary.
- **Storage limitation** – Data must not be kept longer than necessary for the purposes for which it was collected.
- **Integrity and confidentiality** – Data must be processed securely to protect against unauthorised or unlawful processing, loss, destruction, or damage.
- **Accountability** – be able to demonstrate compliance with all principles.

This policy explains how the school ensures compliance with these principles in all aspects of data handling.

6. Data Protection by Design and Default

We integrate data protection into all processing activities by:

- appointing a suitably qualified DPO
- limiting processing to what is necessary
- conducting Data Protection Impact Assessments (DPIAs) where high risk is likely
- embedding privacy in internal documents and notices
- training staff; auditing and reviewing measures
- maintaining records of processing activities and retention schedules.

7. Lawfulness, fairness and transparency

We only use personal information when the law allows us to. There are six main legal reasons for this:

- To deliver what we've agreed with you – for example, providing education or services under a contract.
- To meet our legal duties – such as reporting to the Department for Education.
- To protect someone's vital interests – for instance, in a medical emergency.
- To carry out our public responsibilities – most of what we do as a school falls under this category, like teaching and safeguarding.
- When you've given clear consent – for example, for photos used in newsletters or on social media.
- In very limited cases, for legitimate interests – but as a public authority, we rarely rely on this.

New rules in the Data (Use and Access) Act 2025 also allow schools to use a special basis called "recognised legitimate interests" for certain important purposes, such as safeguarding or preventing crime. We will only use this where it's appropriate and in line with guidance from the Information Commissioner's Office.

For more sensitive information (known as special category data, like health or ethnicity), we follow extra rules set out in the Data Protection Act 2018. Whenever we collect personal data directly from you, we'll explain why we need it and how we'll use it.

8. Collecting, using and sharing personal data

We collect personal information for clear and legitimate purposes, and we explain these purposes in our privacy notices. Staff must only access and use personal data when it is necessary for their role. When information is no longer required, it is securely deleted or anonymised in accordance with our retention schedule.

There are occasions when we need to share personal data. This may include sharing with statutory bodies such as the Department for Education or the Local Authority, with law enforcement agencies where required by law, or with trusted suppliers who provide services to the school (for example, IT support or catering systems). We only work with organisations that can demonstrate compliance with data protection law, and we ensure appropriate contracts or data sharing agreements are in place.

If personal data needs to be transferred outside the UK, we will apply appropriate safeguards to protect it. This includes using approved mechanisms such as adequacy regulations, the UK International Data Transfer Agreement (IDTA), or the UK Addendum to EU Standard Contractual Clauses, and carrying out transfer risk assessments where required.

9. Individual Rights

Under data protection law, individuals have a number of important rights. These include the right to:

- **Access** the personal information we hold about them (often called a Subject Access Request).
- **Correct** any inaccurate or incomplete information.
- **Ask for data to be erased** when it is no longer needed or where consent has been withdrawn.
- **Restrict how data is used** in certain circumstances.
- **Receive a copy of their data** in a portable format.
- **Object** to certain types of processing.
- **Challenge decisions made solely by automated means**, including profiling, with safeguards introduced by the Data (Use and Access) Act 2025.

If anyone wishes to exercise one of these rights, they should contact our Data Protection Officer (DPO) through the school office. Staff must forward any such request to the DPO immediately

10. Subject Access Requests (SARs)

Individuals have the right to request a copy of the personal information we hold about them. This is known as a Subject Access Request (SAR). Requests can be made in writing, verbally, or even through social media. When we receive a SAR, we will:

- **Acknowledge the request promptly** and record it in our SAR log.
- **Verify identity** where necessary, which may include asking for two forms of identification or confirming details by phone.
- **Search for the relevant data** in a reasonable and proportionate way, as required by law.
- **Respond within one month** of receiving the request. If the request is complex or there are multiple requests, we may extend this by up to two months. If an extension is needed, we will inform the individual within the first month and explain why.

- Provide the information **free of charge**, unless the request is clearly unfounded or excessive. In such cases, we may refuse or charge a reasonable fee and will explain the reasons for this decision.

We will not disclose information if doing so could cause serious harm to the physical or mental health of the pupil or another individual, reveal that a child is at risk of abuse, include adoption or parental order records, or relate to court proceedings concerning the child.

If we refuse a request, we will explain why and inform the individual of their right to complain to the Information Commissioner's Office (ICO).

Our full SAR procedure, including detailed steps and forms, is set out in Appendix 4 at the end of this policy.

11. SARs for Children

Personal data about a child belongs to that child, not to their parents or carers. In most cases at Ravenscliffe High School, pupils may not fully understand their data protection rights or the implications of making a Subject Access Request (SAR). For this reason, if a parent or carer makes a SAR on behalf of their child, we will normally allow this, provided it is clearly in the child's best interests.

While the law generally assumes that children aged 12 and above can understand their rights, we recognise that many of our pupils have special educational needs and may not have the capacity to make this decision themselves. Each request will be considered on a case-by-case basis, taking into account the child's level of understanding and welfare.

12. Parental requests to view educational records

Parents or those with parental responsibility are entitled to access their child's educational record**.** An educational record includes almost all the information a school holds about a pupil, such as:

- Teacher reports, assessments, and academic results
- Notes on progress, attendance, and behaviour
- Correspondence with parents, educational psychologists, or Local Authority staff

It does **not** include information held privately by a teacher for their own use or data about another child.

Parents must make a written request, and we will provide access free of charge within 15 school days**, in** accordance with Regulation 5 of the Education (Pupil Information) (England) Regulations 2005**.**

For any personal data not part of the educational record, or if a parent or pupil requests broader access, this will follow the Subject Access Request (SAR) procedure under UK GDPR, as detailed in Appendix 4**.**

13. CCTV, Photographs and Images

To help keep our school site safe and secure, we use CCTV in certain areas. The full arrangements for CCTV, including how footage is managed and stored, are set out in our separate CCTV Policy**.** For GDPR purposes, we follow the ICO's guidance on video surveillance and the Home Office Surveillance Camera Code of Practice, and we ensure clear signage wherever cameras are in use.

We also take photographs and record images as part of school activities. These may be used for communication, marketing, or promotional purposes, such as newsletters, displays, or the school website. We always obtain written consent from parents or carers (or from pupils aged 18 and over) before using images in this way. Consent can be refused or withdrawn at any time, and if it is withdrawn, we will delete the images and stop any further use.

In addition, visual evidence plays an important role in assessing and supporting pupils with special educational needs and disabilities (SEND). Photographs and videos may be used to record progress, demonstrate achievements, and inform personalised learning plans. These images are handled with the same level of care and security as all other personal data, and their use is strictly for educational purposes

14. Disposal of Records

All personal data is retained and disposed of in line with the school's Records Retention Schedule, which sets out how long different types of information are kept and when they should be securely destroyed. This ensures we only keep data for as long as it is needed for legal, educational, or operational purposes.

When personal data is no longer required, or becomes inaccurate, it will be disposed of securely. This may include shredding paper records or permanently deleting and overwriting electronic files. Where we use approved third parties to destroy records, we ensure they provide appropriate guarantees and have contracts in place to meet data protection standards.

15. Managing Personal Data Breaches

Ravenscliffe High School takes every reasonable step to prevent personal data breaches. However, if a breach is suspected, we will act quickly and follow the detailed procedure set out in Appendix 2 of this policy.

Where appropriate, the breach will be reported to the Information Commissioner's Office (ICO) within 72 hours by our Data Protection Officer (DPO). Examples of breaches in a school context may include:

- A non-anonymised dataset being published on the school website, such as exam results for pupils eligible for the pupil premium.
- Safeguarding information being accessed by someone who is not authorised to see it.
- The theft of a school laptop containing unencrypted personal data about pupils.

All staff must report any suspected breach immediately, and no action should be taken outside the procedure outlined in Appendix 2.

16. Training

All staff receive annual training on data protection and GDPR to ensure they understand their responsibilities and follow best practice when handling personal information. In addition, each year staff complete the DfE-recommended cyber security training, which helps protect school systems and data from online threats. This training is refreshed regularly and forms part of our commitment to safeguarding personal data and maintaining compliance with UK GDPR.

17. Links to other policies

- Record retention schedule
- Online Safety Policy
- Safeguarding Policy
- CCTV Policy
- Freedom of Information Policy

18. Monitoring and review

This policy will be reviewed and updated if changes in UK law necessitate a change to school practices. Otherwise, this policy will be reviewed annually and shared with the full governing board.

Appendix 1 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 (not currently being used) • 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.

Appendix 2 – Data Breach Procedure

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

1. On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Head Teacher/Business Manager.
2. The staff member or data processor will be asked to complete the school's data breach form.
3. The Head Teacher/Business Manager will assess the nature of the breach and make an initial entry in the school's breach register.
4. The Head Teacher/Business Manager will inform the DPO of the potential breach
5. On receiving the breach report, 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:

    a. Lost
    b. Stolen
    c. Destroyed
    d. Altered
    e. Disclosed or made available where it should not have been
    f. Made available to unauthorised people

6. The DPO will keep the headteacher informed throughout the process
7. 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.
8. The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
9. 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:

    a. Loss of control over their data
    b. Discrimination
    c. Identify theft or fraud
    d. Financial loss
    e. Unauthorised reversal of pseudonymisation (for example, key-coding)
    f. Damage to reputation
    g. Loss of confidentiality
    h. Any other significant economic or social disadvantage to the individual(s) concerned
    i. If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO within 72 hours of the breach being reported.

10. 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 recorded within the school breach register.
11. 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. A description of the nature of the personal data breach including, where possible:
        i. The categories and approximate number of individuals concerned
        ii. The categories and approximate number of personal data records concerned
    b. The name and contact details of the DPO
    c. A description of the likely consequences of the personal data breach
    d. 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

12. 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
13. 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:

    a. The name and contact details of the DPO
    b. A description of the likely consequences of the personal data breach
    c. 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

14. The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

    a. Facts and cause
    b. Effects
    c. Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

15. Depending on the severity of the breach, the DPO and headteacher will either discuss the outcome over the phone or meet to review what happened and how it can be stopped from happening again. This will happen as soon as reasonably possible.

Appendix 3 – Data Breach Report Form

Data Breach Report Form		
This form should be completed as soon as a data breach has been discovered. Please complete sections 1 -7 with as much information as possible and pass the form on to the School Business Manager or Headteacher immediately. The breach will be recorded on the School's Breach Register and the DPO informed so that an investigation can be carried out		
	Report by:	
	Date	
1	Nature of breach e.g. theft/disclosed in error/technical problem	
2	Description of how the breach occurred:	
3	When was the breach reported and how did you become aware?	
4	Full description of all personal data involved	
5	Number of individuals affected? Have all individuals affected been informed	
6	What immediate remedial action was taken:	
7	Has the data been retrieved or deleted? If yes – date and time:	
8	Any Procedure changes needed to reduce risks of future data loss	
9	Conclusion	

Appendix 4

Subject Access Request Procedure

SUBJECT ACCESS REQUESTS

- An individual can make a subject access request verbally or in writing. It does not need to be to a particular person and can even be requested through social media. It does not need to use the words "subject access request" as long as it is clear that they want their personal data.

- A third party can also ask for a subject access request. Often, this will be a solicitor acting on behalf of a client, but it could simply be that an individual feels comfortable allowing someone else to act for them. In these cases, we will ask for written authority to make the request or a power of attorney. If we deem it appropriate we will send the information to the individual rather that the third party but we can send the information to the third party.

Before responding to a subject access request for information held about a student, we will need be confident they understand their rights before responding directly to them. If a parent is requesting the information on behalf of the child and it is evident that this is in the best interests of the child then we will send the information to the parent.
The following needs to be considered when a student request has been received.

- the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.
- We will respond within a month. If we feel the need to ask for ID, the one month time limit will start once we receive the ID.

ONCE A SAR IS RECEIVED

- Once a request has been received then it will be logged by the DPO in the subject access log. The log needs to record the details of the request and how it was requested.
- We will acknowledge receipt and confirm we have data held within 3 working days. We will send a SAR form to the individual either as a hard copy or electronically. This will ask them what information they would like. We will still respond within a month once we receive the form or if they refuse to complete the form.

INFORMATION SENT AS PART OF THE SAR.

- Confirmation that we are processing their personal data, give them a copy of their own personal data, as well as other supplementary information.
- Privacy Notice
- If pertinent information about the source of the data, where it was not obtained directly from the individual.
- Personal data held on that individual as requested by the SAR form or all personal data held after reasonable searches are made.
- If the data we hold includes disclosing information about another individual we can only send this if:
- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose the information, you must take into account all of the relevant circumstances, including:

- the type of information that you would disclose;
- any duty of confidentiality you owe to the other individual;
- any steps you have taken to seek consent from the other individual;
- whether the other individual is capable of giving consent; and
- any express refusal of consent by the other individual.
- We will look at the data we are sending out and ensure it is clear, any information that it may need explaining i.e. attendance codes will be explained.
- We will send any personal data we hold at the time of responding to the individual. Some data may have been deleted between the request and response as part of normal office procedures.
- If an individual makes a request electronically, we will provide the information by secure e mail, password protected in a zip file, unless the individual requests otherwise.

SCHOOL PROCEDURE TO OBTAIN PERSONAL DATA

Email all teaching staff asking them for any information on the particular subject. They would be asked to either email the information securely to the office or pass hard copies to the office for scanning and collating. This information would include:

1. Paper records
2. Computer records
3. Data bases
4. Photographs.
5. SIMS data base
6. Evolve Data base
7. Assessment information
8. CPOMS?
9. Student file (either paper or electronic)
10. Records Server for EHC Plans/Next Steps/Moving and Handling Plans/Behaviour Plans
11. Team Teach (Behaviour Management) information
12. Accident/Incident Books

REFUSING A SAR

We can refuse a SAR if it is

- manifestly unfounded; or
- excessive.

A request may be manifestly unfounded if:

- the individual clearly has no intention to exercise their right of access. For example an individual makes a request, but then offers to withdraw it in return for some form of benefit from the organisation; or
- the request is malicious in intent and is being used to harass an organisation with no real purposes other than to cause disruption. For example:
- the individual has explicitly stated, in the request itself or in other communications, that they intend to cause disruption;
- the request makes unsubstantiated accusations against you or specific employees;
- the individual is targeting a particular employee against whom they have some personal grudge; or
- the individual systematically sends different requests to you as part of a campaign, e.g. once a week, with the intention of causing disruption.
- A request may be excessive if:
- it repeats the substance of previous requests and a reasonable interval has not elapsed; or
- it overlaps with other requests.
- However, it depends on the particular circumstances. It will **not necessarily** be excessive just because the individual:
- requested a large amount of information, even if you might find the request burdensome. Instead you should consider asking them for more information to help you locate what they want to receive.

- wanted to receive a further copy of information they have requested previously. In this situation a controller can charge a reasonable fee for the administrative costs of providing this information again and it is unlikely that this would be an excessive request;
- made an overlapping request relating to a completely separate set of information; or
- previously submitted requests which have been manifestly unfounded or excessive.
- We will inform the individual as soon as possible and within one month of receipt of the request.
- We will inform the individual about:
- the reasons you are not taking action;
- their right to make a complaint to the ICO or another supervisory authority; and
- their ability to seek to enforce this right through a judicial remedy.

Appendix 5

Ravenscliffe High School and Sports College **Subject Access Request (SAR) Form**	
Section 1 – About the person making the SAR	
Full Name	
Address	
Telephone	
Email	

Section 2 – The subject of the SAR	
Are you the person that the requested data relates to?	Yes/No
If you are not the subject of this access request, please go to Section 3	

Section 3 – Acting on behalf of a child	
Childs Name	Yes/No
Childs Date of Birth	
Your relationship to the child	
Has the child given consent for you to act on their behalf?	Yes/No
Can the child understand their rights and what is in their best interests?	Yes/No

Section 4 – Proof of Identity	
Please provide copies of two forms of identification listed below, highlighting as relevant, and enclose them with your application.	
Passport	Driving License
Birth Certificate	Marriage Certificate
Letter of Authority	Power of Attorney
Other (please state)	

Section 5 – Details of the information requested	
Please indicate below the information that you are requesting. Be as **specific and detailed** as possible; doing so will greatly help the school in collating the requested information which in turn will reduce the time taken to respond to your request. If you can, list specific systems you would like data extracting from, and indicate the timescales of your request.	
Start date of data request:	
End date of data request	
Data Requested	

Section 6 – Declaration	
I confirm that: • I have the authority to make this request and, where applicable, have provided evidence of parental responsibility or consent. • I have read and understood the school's **Data Protection (GDPR) Policy**. • I have completed all sections of this form accurately and to the best of my knowledge. • I understand that under **UK GDPR**, providing clear and specific details about the information requested will help the school process my request promptly. • I acknowledge that, under UK GDPR, if my request is complex or numerous, the school may take up to **three months** to respond instead of the usual one month. I will be informed within the first month if an extension is required	
Signed	
Print Name	
Date	

Section 7 – Return Instructions
Please return this form, and necessary identification documents, in hard copy to: Ravenscliffe High School, Ravenscliffe Close, Skircoat Green, Halifax, HX3 0RZ. Or alternatively, email completed forms and copies of identification documents to: GDPR@ravenscliffe.calderdale.sch.uk