DATA PROTECTION POLICY

Policy control table			
Policy title:		Data Protection Policy	
Author:		Compliance Manager	
Policy Version:		4	
Approved on:			
Approved by:			
Date reviewed:		October 2026	
Document History			
Version	**Date Written**	**Author**	**Note of revisions**
2	**October 2024**	**David Thorpe**	**AI Section added**
3	**June 2026**		**Updated in line with DUAA changes**
4	**July 2026**		**Updated by DPO**

Contents

1. Aims 3
2. Legislation and guidance 3
3. Definitions 3
4. The data controller 5
5. Roles and responsibilities 5
6. Data protection principles 6
7. Collecting personal data 6
8. Sharing personal data 8
9. Subject access requests and other rights of individuals 9
10. Parental requests to see the educational record 11
11. Surveillance Camera Systems (CCTV) 11
12. Photographs and videos 11
13. Artificial intelligence (AI) 12
14. Data protection by design and default 12
15. Data security and storage of records 13
16. Disposal of records 13
17. Personal data breaches 14
18. Data Protection Complaints 14
19. Training 14
20. Monitoring arrangements 14
21. Links with other policies 14
Appendix 1: Personal data breach procedure 15
Appendix 2: Appropriate Policy Document (APD) 18

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents and carers, visitors and other individuals is collected, stored and processed in accordance with the UK data protection law.

This policy applies to all **personal data**, regardless of whether it is in paper or electronic format

2. Legislation and guidance

This policy meets the requirements of the:

- 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)
- The Data (Use and Access) Act 2025 (DUAA)

It is based on guidance and resources published by the Information Commissioner's Office (ICO) on the UK GDPR and a policy paper 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

3. Definitions

TERM	DEFINITION
Personal data	Any information relating to an identified, or identifiable, living individual, whether identified directly or indirectly. This may include the individual's: ● Name (including initials) ● Address and contact details ● Identification numbers such as NI or passport number ● Location data ● Online identifier, such as a username ● Photographs or video footage 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 or facial recognition), where used for identification purposes

	• Health – physical or mental • Sex life or sexual orientation
Processing	Any activity that involves the use of personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual, and also includes transmitting or transferring personal data to third parties.
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. The data controller is responsible for establishing practices and policies in line with the UK GDPR.
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. A data processor acts only on the instructions of the controller and does not determine the purposes or means of the processing.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
Data Protection Officer (DPO)	A named individual who helps the school protect their data and stay compliant with data protection regulations
Information Commissioner's Office (ICO)	The UK supervisory authority for data protection. They have the responsibility for enforcing the data protection regulations (UK GDPR)
UK General Data Protection Regulation (UK GDPR)	The UK GDPR is the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (EU GDPR)
Data Protection Act (DPA) 2018	The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR)
The Data Use and Access Act 2025 (DUAA)	The Data Use and Access Act (DUAA) is UK legislation amending and updating the UK GDPR and the Data Protection Act

4. The data controller

Our school processes personal data relating to parents and carers, pupils, staff, management committee members,, visitors and others. In carrying out these activities, the school acts as a data controller.

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

5. Roles and responsibilities

This policy applies to **all staff and volunteers** should they be employed (paid and unpaid) employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action in line with the school's HR policies..

5.1 Management Committee

The Management Committee has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2 Data protection officer

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

They will provide an annual report of their activities directly to the management committee and, where relevant, report on their advice and recommendations on school data protection issues. The DPO will work closely with the school compliance manager providing expertise, advice and training as a partnership arrangement

The DPO is also the first point of contact for the ICO. For data requests or other queries data subjects would commonly contact the internal lead initially, followed by the DPO when necessary.

Our internal lead for data protection is the Compliance manager, David Thorpe dthorpe@rotherhamaspire.org

Our DPO is **EduDataPro** and is contactable via **dpo@edudatapro.com**.

5.3 Headteacher

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

5.4 All staff

Staff are responsible for:

- Following all school policies
- 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
- Reporting any incidents or breaches to the Compliance manager and/or the DPO in the following circumstances
    - If they have 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 or suspected data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

We adhere to the principles relating to processing of personal data set out in the UK GDPR, which requires personal data to be

- Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency);
- Collected for specified, explicit and legitimate purposes (purpose limitation);
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed (data minimisation);
- Accurate and, where necessary, kept up to date (accuracy);
- Kept for no longer than is necessary for the purposes for which it is processed (storage limitation);
- Processed in a way that ensures it is appropriately secure (security, integrity and confidentiality);
- Not transferred to another country without appropriate safeguards in place (transfer limitation); and
- Handled in a way that respects the rights of data subjects and allows them to exercise those rights (data subject rights and requests)

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (accountability).

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

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of six '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 data needs to be shared with another data controller under a '**recognised legitimate interest**' either to allow them to fulfil their 'public task' obligations or using a 'condition' such as 'safeguarding a vulnerable individual', 'crime', 'emergency', or 'national security'. In this instance anyone under 18 is defined as a 'vulnerable individual'
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing 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 interests** 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 defence 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 or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **public health reasons**, 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, we 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 interests** 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 defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

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

We will always consider the fairness of our data processing. We will ensure we 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.

7.2 Limitation, minimisation and accuracy

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

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

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

We 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 anonymised. This will be done in accordance with the school's record retention schedule.

8. Sharing personal data

We are required to routinely share personal data with our pupils' parents and carers, our local authority, the Department for Education and other schools or colleges to which our pupils transfer when leaving us. The law allows us to do this without relying on consent. In addition we may be required to share personal data with other organisations, agencies or companies for example in situations where:

- There is an issue with a pupil or a parent or carer that puts the safety of our staff at risk
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils. 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 any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service

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

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

In some circumstances we may request consent before sharing personal data.

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

Further details of how we share data can be found in our privacy notice for staff parents and students (located on our school website).

We will not share personal data in training sessions, CPD or any presentations. Any case histories will ensure that the subject remains anonymous.

9. Subject access requests and other rights of individuals

9.1 Subject access requests (SARs)

By law individuals have a right to make a 'subject access request' (SARs) 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 isn't possible, the criteria used to determine this 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 data controller or the ICO
- 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:

- The name of 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 forward it to the compliance manager

9.2 Children and subject access requests

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

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request (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 2 or 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.
- If we are waiting for clarification or proof of ID etc from the requester then we may 'stop the clock' until this information is received.

We 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. If the required searches to fulfil the request are not 'reasonable and proportionate' then we may refuse the request or ask that the search scope be reduced.

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 legal processes.

9.4 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 (where they have provided consent and subject to restrictions imposed by legal obligations on the Data Controller)
- 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 personal data breach (in certain circumstances)

- Make a complaint to the data controller and/or 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 Compliance manager and if staff receive such a request, they must immediately forward it to the Compliance manager who will forward to the DPO and conduct a meeting before proceeding.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it.

This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced

11. Surveillance Camera Systems (CCTV)

We use surveillance cameras (also known as CCTV) in various locations around the school site to ensure it remains safe. We will follow the ICO's guidance for the use of CCTV systems and comply with data protection principles.

We do not need to ask individuals' permission to use surveillance cameras, but we make it clear where individuals are being recorded. Cameras are clearly visible and accompanied by prominent signs explaining that cameras are in use.

Any enquiries about the CCTV system should be directed to the compliance manager.

There is a CCTV/Surveillance policy in place and available to all members of staff and the management committee.

12. Photographs and videos

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

We will obtain written consent from parents/carers, for pupils under 13 and over 13 years of age. Pupils over the age of 13 may also be asked for their own consent (unless they are deemed not "Gillick Competent"),

This applies to photographs and videos of pupils to be used for communication, marketing and promotional materials only.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parents/carers and the pupil.

Parents/carers are not allowed to take photographs at school events for their own personal use as they are not covered by data protection legislation, unless specifically requested beforehand and agreed by the Head Teacher. Any such photos or videos with other pupils must not be shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.

Where the school takes photographs and videos, uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

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

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

See our safeguarding policy and electronic communications acceptable use policy for more information on our use of photographs and videos.

13. Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative tools such as ChatGPT, Microsoft Co-pilot and Google Gemini. Our school 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 school will treat this as a data breach, and will follow the personal data breach procedure outlined in appendix 1.

14. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge supported by and in conjunction with the Compliance manager
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing data protection impact assessments (DPIAs) where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance (Annual training is scheduled into the CPD diary)
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws will apply
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school, the compliance manager and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure

15. Data security and storage of records

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

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access
- Where it is necessary to remove hard-copy personal information from Rotherham Aspire premises, staff must record the documents as signed out and subsequently signed back in using the designated form on the shared system. This requirement applies to documents taken to external meetings or to a staff member's home. Documents containing personal information must be appropriately secured and must not be left unattended in vehicles at any time.
- Documents transferred directly between the four Rotherham Aspire sites are exempt from the sign-in/sign-out requirement, as such transfers are regarded as taking place within Rotherham Aspire's secure operational perimeter. Staff must nevertheless maintain the security of the information throughout transit. If a stop is made during the journey, documents must not be left unattended in the vehicle.
- Where hard copy personal information needs to be taken off site, staff must sign it in and out on the form provided on the shared system. This includes documents being to meetings or to staff member's homes. Documents must not be left unattended in cars. This excludes documents being transferred between the four Aspire sites. This is regarded as within the safe perimeter of Rotherham Aspire. However, when traveling between sites documents must not be left in cars should a stop occur.
- Passwords made up of 3 random words or are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or management committee members who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our (see our electronic communications – acceptable use policy)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

16. Disposal of records

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

For example, we employ are company to remove paper-based records that are confidential waste from our secure storage or confidential waste bins and take it away to incinerate, we also employ a policy to overwrite or delete electronic files. If we require the third party to provide sufficient guarantees that it complies with data protection law when removing our confidential waste.

17. Personal data breaches

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

In the event of a suspected or confirmed data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. We will also notify the data subject where we are legally required to do so.

18. Data Protection Complaints

We take any complaints about how we collect and use personal data very seriously.

Data Protection complaints will be managed in line with the provisions of the Data (Use & Access) Act 2025. Data Subjects are required to first complain directly to the Data Controller (the school).

The school will

- Acknowledge your complaint within 30 days
- Respond without undue delay, keeping you updated on progress.

If you are not satisfied, you can escalate your complaint to the Information Commissioner's Office (ICO) for a ruling. To make a complaint, please contact the school office by email, with details of your complaint, or speak to the school office about alternative ways of submitting your complaint.

19. Training

All staff are provided with data protection training as part of their induction process. All members of the management committee are required to provide evidence of data protection training.

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

20. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy in line with the Compliance manager.

This policy will be reviewed annually and approved by the management committee

21. Links with other policies

This data protection policy is linked to our:

- Freedom of information process
- Electronic Communications – Acceptable use policy
- Staff code of conduct
- CCTV policy
- Safeguarding policy

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

- On finding or causing a breach, or potential breach, the staff member, management committee member or data processor must immediately notify the compliance manager, data protection officer (DPO) or head teacher.
- The DPO/compliance manager will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- Staff and management committee members will co-operate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation
- If a breach has occurred or it is considered to be likely that is the case, the compliance manager and/or DPO will alert the headteacher and the chair of the management committee
- The DPO/compliance manager will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO/compliance manager with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types at the end of this procedure)
- The DPO/compliance manager will assess the potential consequences, based on how serious they are, and how likely they are to happen before and after the implementation of steps to mitigate the consequences
- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool
- The DPO/compliance manager will document the decisions (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school's computer system
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach

- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the school's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible. The DPO will be supported by the compliance manager with this process

- Where the school is required to communicate with individuals whose personal data has been breached, the DPO/compliance mangager will tell them in writing. This notification will set out:

    - A description, in clear and plain language, of the nature of the personal data breach

    - The name and contact details of the DPO/compliance manager

    - A description of the likely consequences of the personal data breach

    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

- The DPO/compliance manager will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

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

    - Facts and cause

    - Effects

    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be stored on the school's computer system

- The DPO, compliance manager and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

- The DPO and the compliance manager will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches

Example actions to minimise the impact of data breaches

The trust will follow the steps below:

1. **Identification**: To identify what has happened and what personal and other sensitive data is affected
2. **Containment**: To contain and limit the impact of the breach and recover any personal data
3. **Risk assessment**: To assess the risks caused by the breach, especially to individual data subjects
4. **Inform**: To inform data subjects so that they are aware and can take any necessary action
5. **Report**: To report to the ICO, if the breach is considered to have reached the threshold for reporting, or to log the incident on school systems

We will take the actions set out below to mitigate the impact of different types of data breach. We will review the effectiveness of these actions and amend them as necessary after any data breach.

- Investigate school systems to confirm the source of the breach.
- Interview staff and pupils to investigate the reason for the breach. (eg. malicious or accidental)

- Contact recipients of data and request that the data in question is deleted, and not shared, published or replicated, and evidence of this action is provided (eg. screenshot of deletion)
- Attempt to remotely wipe a lost or stolen school phone or other device
- Carry out searches to check if the information has been made publicly available.
- Log requests with internet based providers to remove copies of any breached data.
- Change login credentials for any compromised accounts
- Document actions and outcomes.

Appendix 2: Appropriate Policy Document (APD)

Our processing of special categories of personal data and criminal offence data

As part of our schools functions, we process special category data and criminal offence data in accordance with the requirements of Article 9 and 10 of the General Data Protection Regulation ('GDPR') and Schedule 1 of the Data Protection Act 2018 ('DPA 2018').

Special category data

Special category data is defined at Article 9 UK GDPR as personal data revealing:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric data for the purpose of uniquely identifying a natural person;
- Data concerning health; or
- Data concerning a natural person's sex life or sexual orientation

It is also important to be aware that some of the nine protected characteristics outlined in the Equality Act 2010 are classified as special category data. These include **race**, **religion** or **belief**, and **sexual orientation**. They may also include **disability**, **pregnancy**, and **gender reassignment** in so far as they may reveal information about a person's **health**.

Criminal conviction data

Article 10 UK GDPR covers processing in relation to criminal convictions and offences or related security measures. In addition, section 11(2) of the DPA 2018 specifically confirms that this includes personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing. This is collectively referred to as 'criminal offence data'.

This policy document

Some of the Schedule 1 conditions for processing special category and criminal offence data require us to have an Appropriate Policy Document ('APD') in place, setting out and explaining our procedures for securing compliance with the principles in Article 5 and policies regarding the retention and erasure of such personal data.

This document explains our processing and satisfies the requirements of Schedule 1, Part 4 of the DPA 2018.

In addition it provides some further information about our processing of special category and criminal offence data where a policy document isn't a specific requirement. The information supplements our privacy notices which are available on the school/trust website here. [link to privacy notices]

Conditions for processing special category and criminal offence data

We process special categories of personal data under the following UK GDPR Articles:

1. Article 9(2)(b) – where processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the [school/trust] or the data subject in connection with **employment,** social security or social protection.

Examples include our processing of staff sickness absences.

2. Article 9(2)(g) - reasons of **substantial public interest**.

   The school/trust is a public body. Our processing of personal data in this context is for the purposes of substantial public interest and is necessary for the carrying out of our role.
   An example of this processing would include sharing special category data with the DfE when required, for example as part of the school census.

3. Article 9(2)(j) – for **research** purposes in the public interest.

   The relevant purpose we rely on is Schedule 1 Part 1 paragraph 4 – research.

   An example of our processing is working with universities and the Department of
   Education to provide data for research purposes to help improve UK schools and education.

4. Article 9(2)(h) – the treatment or the **management of health**.

   Examples include our processing of data received from an NHS professional or other healthcare worker about one of our pupils.

5. Article 9(2)(i) – for reasons of public interest in the area of **public health**.

   Examples include our sharing data about our staff or pupils with the NHS in the case of a pandemic.

6. Article 9(2)(a) – **explicit consent**

   In circumstances where we seek consent, we make sure that the consent is unambiguous and for one or more specified purposes, is given by an affirmative action and is recorded as the condition for processing.

   Examples of our processing include information about student or staff dietary requirements, allergies and other health information that we require to look after the wellbeing of our pupils and workforce.

   When we ask for ethnicity (requested by the DfE for school census returns) we make it clear that providing it is optional and by providing it the data subject (or their parent/carer) is consenting for it to be shared with the DfE.

7. Article 9(2)(c) – where processing is necessary to protect the **vital interests** of the data subject or of another natural person.

   An example of our processing would be using health information about a student or member of staff in a medical emergency.

We process criminal offence data under Article 10 of the UK GDPR

Examples of our processing of criminal offence data include pre-employment checks (DBS, barred list) and declarations by a member of the school/trust workforce in line with contractual or safeguarding obligations.

Processing which requires an Appropriate Policy Document

Almost all of the substantial public interest conditions in Schedule 1 Part 2 of the DPA 2018, plus the condition for processing employment, social security and social protection data, require an APD (see Schedule 1 paragraphs 1 and 5).

This section of the policy is the APD for the school. It demonstrates that the processing of special category ('SC') and criminal offence ('CO') data based on these specific Schedule 1 conditions is compliant with the requirements of the UK GDPR Article 5 principles. In particular, it outlines our retention policies with respect to this data.

Description of data processed

- Health and medical data - workforce and pupils
- Ethnicity - pupils and workforce
- Religion - pupils and workforce
- Trade union membership - staff
- Criminal records - DBS checks for all members of the school workforce (paid and unpaid)

Further information about this processing can be found in our privacy notices.

We also maintain a record of our processing activities in accordance with Article 30 of the UK GDPR.

Schedule 1 conditions for processing

Special category data

We process SC data for the following purposes in Part 1 of Schedule 1:

- **Paragraph 1(1)** employment, social security and social protection.

We process SC data for the following purposes in Part 2 of Schedule 1. All processing is for the first listed purpose and might also be for others dependent on the context:

- **Paragraph 6(1) and (2)(a)** Statutory etc and government purposes
- **Paragraph 8(1) and (2)** Equality of opportunity or treatment
- **Paragraph 18(1)** Safeguarding of children and of individuals at risk

Criminal offence data

We process criminal offence data for the following purposes in parts 1 and 2 of Schedule 1:

- **Paragraph 1** – employment, social security and social protection

Procedures for ensuring compliance with the principles

Accountability principle

We have put in place appropriate technical and organisational measures to meet the requirements of accountability. These include:

- The appointment of a data protection officer who reports directly to our highest management level.
- Taking a 'data protection by design and default' approach to our activities.
- Maintaining documentation of our processing activities.

- Adopting and implementing data protection policies and ensuring we have written contracts in place with our data processors.
- Implementing appropriate security measures in relation to the personal data we process.
- Carrying out data protection impact assessments for our high risk processing.

We regularly review our accountability measures and update or amend them when required.

Principle (a): lawfulness, fairness and transparency

Processing personal data must be lawful, fair and transparent. It is only lawful if and to the extent it is based on law and either the data subject has given their consent for the processing, or the processing meets at least one of the conditions in Schedule 1.

We provide clear and transparent information about why we process personal data including our lawful basis for processing in our privacy notice, staff privacy notice and this policy document.

Our processing for purposes of substantial public interest is necessary to function as a school/trust under the Education Act 2005

Our processing for the purposes of employment relates to our obligations as an employer.

We also process special category personal data to comply with other obligations imposed on the school/trust by the Department for Education or our local authority.

Principle (b): purpose limitation

We process personal data for the purposes explained above when the processing is necessary for us to fulfil our statutory functions as a [school/trust]

If we are sharing data with another controller, we will document that they are authorised by law to process the data for their purpose.

We will not process personal data for purposes incompatible with the original purpose it was collected for.

Principle (c): data minimisation

We collect personal data necessary for the relevant purposes and ensure it is not excessive. The information we process is necessary for and proportionate to our purposes. Where personal data is provided to us or obtained by us, but is not relevant to our stated purposes, we will erase it.

Principle (d): accuracy

Where we become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure that data is erased or rectified without delay. If we decide not to either erase or rectify it, for example because the lawful basis we rely on to process the data means these rights don't apply, we will document our decision.

Principle (e): storage limitation

All special category data processed by us for the purpose of employment or substantial public interest is retained for the periods set out in our retention schedule

We determine the retention period for this data based on our legal obligations and the necessity of its retention for our business needs. Our retention schedule is reviewed regularly and updated when necessary.

Principle (f): integrity and confidentiality (security)

Electronic information is processed within our secure network. Paper copies of personal data are kept locked in filing cabinets in locked offices.

Our electronic systems and physical storage have appropriate access controls applied, only relevant staff have access to the files.

The systems we use to process personal data allow us to erase or update personal data at any point in time where appropriate.

Retention and erasure policies

Our retention and erasure practices are set out in our retention schedule which is available on request from the school office

APD review date

This policy will be retained for the duration of our processing and for a minimum of 6 months after processing ceases.

This policy will be reviewed **annually** or revised more frequently if necessary.

Additional special category processing

We process special category personal data in other instances where it is not a requirement to keep an appropriate policy document. Our processing of such data respects the rights and interests of the data subjects. We provide clear and transparent information about why we process personal data including our lawful basis for processing in our privacy notice and workforce privacy notice.