DATA PROTECTION POLICY
Including AI, CCTV and Photos

Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018 as amended post Brexit)

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

Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

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

Data protection in schools - Generative artificial intelligence (AI) and data protection in schools - Guidance - GOV.UK

Guidance on AI and data protection | ICO

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 Category Personal Data	Personal data which is more sensitive and so needs more protection, including information about an individual's: o a safeguarding matter o pupils in receipt of pupil premium o pupils with special educational needs and disability (SEND) o children in need (CIN) o children looked after by a local authority (CLA) o 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 ○ Gender / 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 person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.

The data controller

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

Roles and responsibilities

This policy applies to **all staff** 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.

Governing body

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

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 governing body and, where relevant, report to the board their advice and recommendations on school data protection issues.

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

Our DPO is Naomi Drapkin and is contactable via the school office

Headteacher

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

All staff

Staff are responsible for:

1. Collecting, storing and processing any personal data in accordance with this policy
2. Informing the school of any changes to their personal data, such as a change of address
3. Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals o If they need help with any contracts or sharing personal data with third parties

Data protection principles

The GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner

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

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

Collecting personal data

Lawfulness, fairness and transparency

We will only process personal data where we have one 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 e.g. 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,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school 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**

Special category data will only be processed where an additional Article 9 condition applies. Privacy notices clearly explain how and why data is processed. Individuals have the right to withdraw their consent at any time, and we will ensure that withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal.

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 to do their jobs.

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

management policy.

Records of Processing Activities (Article 30)

A **Data Protection Impact Assessment (DPIA)** will be completed where processing is likely to result in a high risk to individuals' rights and freedoms, including:

- Use of new technologies
- CCTV or surveillance changes
- Use of AI tools involving personal data
- Profiling or large-scale processing of special category data

Data Sharing and Third Parties

Personal data is only shared where lawful, necessary, and proportionate. All processors must provide sufficient guarantees of GDPR compliance and be subject to a written Data Processing Agreement.

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

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We 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 and comply with our safeguarding duties to our staff and pupils – for example, IT companies (including filtering and monitoring.

When doing this, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

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

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

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.

Where we transfer personal data to a country or territory outside the country, we will do so in accordance with data protection law.

Subject access requests and other rights of individuals

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 isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- The existence of a right to request rectification or erasure of personal data or restriction of processing or to object to the processing
- The right to lodge a complaint with the Information Commissioner's Office
- Details of the safeguards in place for any transfers of their data to locations overseas.

Subject access requests must be submitted in writing, either by letter, email or fax to the DPO. They should include:

1. Name of individual
2. Correspondence address
3. Contact number and email address
4. Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO.

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 12 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.

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 he request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual 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

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

While children under 12 are generally not considered mature enough to understand SAR implications, we will assess each case individually based on the child's capacity and understanding, following the guidance of the Gillick competence principle.

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, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or

profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need 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.

Any enquiries about the CCTV system should be directed to the school office.

These key principles apply to our use of CCTV:

- Lawful Basis: We have a clear and lawful basis for using CCTV. This is ensuring the safety and security of pupils, staff, and property.
- Transparency: We inform individuals that they are being recorded. This will be done through clear signage and privacy notices.
- Data Minimization: Only the necessary amount of personal data will be collected. Cameras will be positioned to avoid capturing more footage than needed.

Retention Period: CCTV footage will be retained only for as long as necessary. We follow the ICO recommendation of a retention period of up to 31 days unless the footage is required for an ongoing investigation.

- Access and Security: Access to CCTV footage will be restricted to authorized personnel only. The footage will be stored securely to prevent unauthorized access.
- Data Subject Rights: Individuals have the right to access their personal data recorded by CCTV under a SAR.

Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school for printed materials such as a prospectus or marketing materials. We will clearly explain how the image will be used to both the parent/carer

and pupil.

We do this under the lawful basis of legitimate interest.

We will inform and give a chance to opt out from parents/carers (and children over 12) for photographs and videos to be taken of their child for communication, marketing and promotional materials. Opt out can be exercised at any time. We will then 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. We will get consent to share photos on any online sites. If we use a photo of a pupil, we will not include their name unless we have specific consent to do so.

We will only use a photo in line with the consent provided and for the length of time stated. Consent for photographs and videos will be obtained via a clear, written consent form at the start of each academic year or upon pupil admission, with parents/carers and pupils (where appropriate) fully informed about the intended use and their right to opt out at any time

Photos used in identity management systems may be essential for performing the public task of the school, but we will delete them once a child is no longer a pupil at your school.

The use of photographs and videos is in accordance with The Taking of Photographs Guidance as issued by the ICO.

Use of Artificial Intelligence (AI)

Overview

The use of Artificial Intelligence (AI) technologies within the school environment introduces specific data protection risks that must be carefully managed. These risks relate to how AI systems collect, process, store, and generate information. The school is committed to ensuring that all AI use complies fully with UK data protection legislation, the school's own data privacy policies, and wider safeguarding responsibilities.

All staff will receive training, where relevant, on the data protection risks and ethical considerations of AI use in the school to ensure informed and responsible use.

Risks Related to Personal Data

AI tools often learn from the data entered them. As a result:

- No personal or identifiable data about pupils, parents, or staff should be entered into generative AI tools unless there is a clear, lawful purpose and strict safeguards are in place.

- If personal data must be used, the school will ensure that processing complies with the UK GDPR, including transparency, minimisation, and purpose limitation requirements.
- Staff must never upload pupil work, behavioural information, assessment data, or any other identifiable material into AI systems unless explicit authorisation has been granted and appropriate consent has been obtained where required.

Risks of Inaccurate or Harmful Outputs

AI tools may produce:

- content that is factually incorrect, misleading, or fabricated ("hallucinations"),
- content that appears credible but contains harmful, biased, discriminatory, or inappropriate information,
- outputs that could be used to deceive others (e.g., plausible but fake school communication).

These risks mean staff and students must critically evaluate AI-generated information, and AI outputs must not be treated as authoritative without verification from reliable sources.

Risks of Security Breaches

AI tools—particularly free or cloud-based services—may:

- store input data on external servers beyond the school's control,
- use input data to train models unless an opt-out is available,
- introduce vulnerabilities if not vetted for security and data-handling safeguards.

The school will only use AI tools that have undergone appropriate security checks and have clear, compliant data-handling practices.

Automated Decision-Making and Profiling

Where AI tools are used for analysis, assessment support, or workflow automation:

- The school will remain transparent about any AI-driven processing that involves pupils or parents.
- Pupils and families will be informed where AI plays a role in decision-making about them.
- AI will not be used to make final or high-impact decisions about any pupil; all decisions remain under human control.
- Any consideration of AI-driven profiling will be subject to a Data Protection Impact Assessment (DPIA).

Intellectual Property and Copyright Risks

AI use may create risks relating to ownership and rights over:

1. student work,
2. teacher-created materials,
3. prompts or content entered into AI systems.

Schools must ensure they do not upload or reuse copyrighted materials without permission, and must avoid allowing student work to be used to train AI systems unless lawful consent or a legitimate exception applies.

Bias, Fairness, and Ethical Risks

AI systems may replicate or amplify societal or dataset biases, which can negatively affect pupils with protected characteristics. The school will:

- evaluate AI systems for fairness before use,
- monitor outputs for bias,
- take action where AI creates or reinforces unfair treatment.

Incident Reporting

All AI-related incidents—including data breaches, inappropriate outputs, or suspected misuse—must be reported immediately through the school's established safeguarding and data breach procedures. Incidents may be escalated to external authorities where required.

Ongoing Risk Assessment

AI risk management will align with the school's broader safeguarding, cyber security, and data protection frameworks. Risk assessments will consider:

- legal and ethical factors,
- data protection compliance,
- cyber security posture,
- risks of fraud or impersonation,
- potential impacts on pupil wellbeing.

The school will periodically update its assessments to reflect new research, emerging threats, and changing technology.

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
- 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)
- Integrating data protection into internal documents including this policy, any

related policies and privacy notices
- Periodically 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
- Maintaining records of our processing activities, including:
  - For the benefit of data subjects, making available the name and contact details of our school 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, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

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 are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices.
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment
- 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.

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 will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Personal data breaches

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

In the unlikely event of a suspected 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. Such breaches in a school context may include, but are not limited to:

- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

Training

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

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

Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed **every 2 years** and shared with the full governing board.

Appendix 1: Personal data breach procedure

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

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO

- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully

  - Lost
  - Stolen
  - Altered
  - Destroyed
  - Disclosed or made available when it should not have been

- The DPO will alert the headteacher and the chair of governors

- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)

- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen

- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

  - Loss of control over their data
  - Discrimination
  - Identity theft or fraud
  - Financial Loss
  - Unauthorised use
  - Reputational damage
  - Loss of confidentiality

  Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the schools computer system

- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO

will set out:

- A description of the nature of the personal data breach including, where possible: The categories and approximate number of individuals concerned

  The categories and approximate number of personal data records concerned o The name and contact details of the DPO

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

 If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

 The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

 The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

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

- Facts and cause o 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 schools computer system

- The DPO 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

Actions to minimise the impact of data breaches

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

Sensitive information being disclosed via email (including safeguarding records)

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

Appendix 2: Example template for a letter to parents and carers about record-checking and consent

Child's name:

Date:

Dear [parent/carer name],

Caring for your information

To meet the requirements of UK General Data Protection Legislation (UK GDPR) and best practice, we'd like to take the opportunity to do two things:

1. **Check the accuracy of your child's information**

Firstly, we would like to check that the information we hold about your child, including emergency contact details, is fully up to date. Please see the attached print-out of your child's information from our systems.

2. **Seek your consent to use that information**

Secondly, we use information about your child in a number of ways, and we'd like your consent for some of the ways we use this personal data. We set these out in more detail below.

If you're not happy for us to use your child's information in the ways we list, that's no problem – we'll accommodate your preferences. Similarly, if you change your mind at any time, you can let us know by emailing [email address], calling [phone number], or popping into the school office.

Please take this opportunity to discuss the options with your child.We will review your consent every [period of time, for example, each September].

If you have any other questions, please do get in touch.

Yours sincerely

Headteacher

OFFICE USE ONLY: Insert pupil number as header

Please tick (✓) the relevant box, sign and return to the school office by [date]

1. Accuracy of your child's information

Confirmation	Yes	No
I've checked the print-out of my child's information, including the emergency contact information, and confirm the details are correct (or, where incorrect, I've corrected it).		

2. My consent

Confirmation	Yes	No
I'm happy for the school to take photographs of my child to use on [for example, the school website, school prospectus, or social media – have a separate box for each]		
I'm happy to receive [for example, marketing materials, newsletters or fundraising requests from the school or the parent teacher association (PTA)]		
I understand that I can withdraw my consent at any time		

Signature **Parent/carer signature**	
Parent's/carer's name	
Name of child	
Date	

REGISTER OF PROCESSING ACTIVITIES (adjust to suit school)

Ref	Processing Activity	Data Subjects	Categories of Personal Data	Special Category Data (Y/N – specify)	Purpose of Processing	Lawful Basis (Art. 6)	Art. 9 Condition (if applicable)	Data Source	Data Sharing / Recipients	International Transfers (Y/N)	Retention Period	Security Measures	DPIA Required (Y/N)	Review Date	Notes / Actions
01	Pupil admissions & education records	Pupils	Name, DOB, address, UPN, attendance, attainment	Yes – SEND, safeguarding, health	Provide education and meet statutory duties	Contractual obligation	Safeguarding, Vital interests	Parents / previous school / LA	Local Authority, DfE, exam boards	No	As per IRMS/DfE schedule	role-based access, encryption, staff training	No		Reviewed annually
02	Staff HR and payroll	Staff	Name, address, NI number, bank details, salary	Yes – health, DBS, equality data	Employment administration and payroll	Legal obligation (Art. 6(1)(c))	Employment law obligations (Art. 9(2)(b))	Staff member	Payroll provider, HMRC, pension scheme	No	6 years after employment ends	Secure HR system, limited access, processor contracts	No		Processor contracts reviewed annually
03	CCTV monitoring	Pupils, staff, visitors	Video images	Potential biometric data	Safeguarding and site security	Legitimate interests – Art. 6(1)(f)	Safeguarding DPA 2018	CCTV cameras	Police (if required)	No	31 days	Restricted access, secure storage	Yes		DPIA required and completed
04	Safeguarding and child protection records	Pupils	Safeguarding concerns, referrals, reports	Yes – safeguarding, health	Safeguard children and meet statutory duties	Legal or vital intrests (if urgent)art 6(1) c or d	Safeguarding DPA 2018	Staff / external agencies	Local Authority, social care, police	No	Until child is 25	Restricted access, encryption	Yes		DPIA recommended
05	SEND records and provision	Pupils	EHCPs, assessments, support plans	Yes – health, SEND	Provide SEND support	Legitimate interests – Art. 6(1)(f)		Parents / LA	Local Authority	No	As per SEND retention	Secure , limited access	No		
06	Medical and first aid records	Pupils	Medical conditions, care plans	Yes – health	Ensure pupil health and safety	Vital interests (Art.6(1)(d))	Health care provision	Parents / healthcare	NHS, emergency services	No	DOB + 25 years	Locked cabinets, secure system	No		
07	Attendance monitoring	Pupils	Attendance marks, absence reasons	No	Meet statutory attendance duties	Legitimate interests – Art. 6(1)(f)	N/A	Staff / parents	Local Authority, DfE	No	As per attendance guidance	Attendace system controls	No		
08	Behaviour and exclusions	Pupils	Behaviour logs, exclusion records	Yes – safeguarding	Manage behaviour and discipline	Legitimate interests – Art. 6(1)(f)		Staff		No	As per guidance	Restricted access	No		

09	Assessment and progress tracking	Pupils	Assessment scores, teacher judgements	No	Monitor progress and attainment	Legitimate interests – Art. 6(1)(f)	N/A	Teachers	DfE (statutory returns)	No	As per retention	Secured files	No		
10	Parent communications	Parents	Names, contact details	No	Communicate with parents	Legitimate interests – Art. 6(1)(f)	N/A	Parents	Email/SMS provider	No	While pupil on roll	Secure platforms	No		
11	School trips and activities	Pupils	Consent forms, risk info	Yes – medical	Organise trips safely	Legitimate interests – Art. 6(1)(f)	Vital interests	Parents	Trip providers	No	1 year after trip	Secure storage	No		
12	Admissions appeals	Parents /pupils	Application and appeal documents	No	Manage admissions appeals	Legitimate interests	Consent where required	Parents	Governors, third party mediation	No	As per admissions code	Secure files	No		
13	Complaints handling	Parents /staff	Complaint records	Yes – may include sensitive	Investigate complaints	Contractual obligation		Complainant	Governors, third party mediation	No	6 years	Restricted access	No		
14	Website and communications	Pupils/ staff	Photos, names (where consented)	Yes – images	Promote school	Legitimate interests	Consent where required	School	Public	No	Until withdrawn	Consent controls	No		
15	ICT systems and user accounts	Pupils/ staff	Usernames, activity logs	No	Provide ICT access	Legitimate interests	N/A	School	IT providers	No	Account lifetime	Access controls	No		
16	Filtering and monitoring	Pupils/ staff	Internet usage logs	Potentially	Safeguarding	Legitimate interests	Safeguarding	IT systems	IT provider	No	As per policy	Restricted access	Yes		
17	Governance records	Governors	Contact details, DBS	Yes – DBS	Governance	Legal obligation	Employment law	Governor	LA/DBS service	No	6 years	Secure storage	No		
18	Finance and payments	Parents	Payment records	No	Manage school finances	Legal obligation	N/A	Parents	Payment provider	No	6 years	Secure systems	No		
20	Alumni records	Former pupils	Names, contact info	No	Maintain alumni links	Legitimate interests	N/A	Pupils	Alumni association, governors	No	Until opt-out	Secure database	No		



DPIA— Safeguarding & Child Protection Processing

1. Description of the processing

The school processes personal and special category data relating to safeguarding and child protection concerns, including allegations, referrals, risk assessments, and multi-agency correspondence. Processing is carried out by designated safeguarding staff and stored securely.

2. Purpose of the processing

- To safeguard children and promote their welfare
- To comply with statutory safeguarding duties
- To enable appropriate referrals to external agencies

3. Lawful basis (Article 6)

- **Independent school:**
  Legal obligation – Article 6(1)(c)
  (Education Act 2002, Keeping Children Safe in Education)
- **Alternative (where applicable):**
  Vital interests – Article 6(1)(d)

4. Special category condition (Article 9)

- **Article 9(2)(g)** – Substantial public interest
- DPA 2018 Schedule 1, Part 2 (Safeguarding of children)

5. Data subjects

- Pupils
- Occasionally parents, staff, or third parties

6. Data categories

- Safeguarding concerns
- Social care information
- Health and wellbeing data
- Allegations and referrals

7. Data sharing

- Local Authority (children's social care)
- Police
- Health professionals
- Other safeguarding partners

8. Retention

- In line with statutory safeguarding guidance
- Typically **until the child is 25 years old**

9. Risks to individuals

- Unauthorised access
- Accidental disclosure
- Emotional distress
- Reputational harm

10. Risk mitigation measures

- Restricted access (DSL only)
- Secure systems / locked storage
- Staff safeguarding and GDPR training
- Clear breach procedures

11. Outcome

✓ Risks are **necessary, proportionate, and mitigated**

✓ Processing is lawful and justified

✓ DPIA **approved**

DPIA— CCTV

1. Description of the processing

The school operates CCTV systems to monitor specific areas of the site for safeguarding, safety, and security purposes. Footage is recorded, stored securely, and accessed only by authorised staff.

2. Purpose of the processing

- Safeguarding pupils and staff
- Preventing and detecting crime
- Protecting school property

3. Lawful basis (Article 6)

- **Independent school:**
  Legitimate interests – Article 6(1)(f)
  (Balancing test required)

Public task **does not normally apply** to independent schools for CCTV.

4. Legitimate Interests Assessment (summary)

- **Interest:** Safety and security
- **Necessity:** CCTV is effective and proportionate
- **Balance:** Minimal intrusion; clear signage; limited retention

Legitimate interests justified

5. Special category data

- Potential incidental biometric data (images)
- Condition: **Article 9(2)(g)** – substantial public interest

6. Data subjects

- Pupils
- Staff
- Visitors

7. Data sharing

- Police (only where required)

8. Retention

- **Up to 31 days**, unless required for investigation

9. Risks to individuals

- Excessive surveillance
- Inappropriate access
- Function creep

10. Risk mitigation measures

- ICO-compliant signage
- Restricted access
- Defined retention period
- DPIA reviewed annually

11. Outcome

CCTV use is **lawful, proportionate, and transparent**