Data Protection Policy

Pike Fold Primary School

August 2024

Issue Status

Date	Issue	Date Approved by Governors	Review Date
April 2018	Version 1		Spring 2020
June 2020	Version 2 – reviewed & updated by Global Policing		Summer 2022
May 22	Version 3 – reviewed & updated by RADCaT Ltd due to Brexit		Summer 2024
August 2024	Version 4	September 2024	August 2026

Contents

1. 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 UK General Data Protection Regulation (UK-GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018).

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

2. Legislation & Guidance

This policy meets the requirements of the UK-GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the UK-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. For further information on how Pike Fold Primary School operate CCTV, please refer to our CCTV policy on the school website.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's:

	• Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The Data Controller

Pike Fold Primary School processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is 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 & Responsibilities

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

5.1. Governors

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

5.2. Data Protection Officer (DPO)

The 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 board 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.

The school has an independent data protection officer service supplied by RADCaT Limited, an organisation run by risk management and prevention specialists who work with the school on all aspects of data compliance. If you have any questions or comments, or wish to make any requests under the Regulations, you should contact them directly:

T: 01942 590 785 | E: Danielle.eadie@radcat.co.uk | W: www.radcat.co.uk

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:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the 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 United Kingdom or areas that fall outside of the UK's adequacy agreement.
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6. Data Protection Principles

The UK-GDPR in conjunction with the DPA 2018 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

In addition, Pike Fold Primary School must actively demonstrate 'accountability' and keep records of how the school complies with the key principles.

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

7. Collecting Personal Data

7.1. Lawfulness, Fairness & 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**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the UK-GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

Further information about our lawful bases for processing for certain categories of data can be found in the school privacy notices located at:

- Pupil / Parent Privacy Notice: school website or office
- Staff Privacy Notice: school system or office
- Visitor Privacy Notice: school website or office
- Recruitment Privacy Notice: school website, job application site or office
- Governor Privacy Notice: School website or office

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 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 Record Management Policy and Retention Schedule.

8. Sharing Personal Data

As an education provider, the school has a statutory obligation to share data with the Local Authority and Department for Education. Data about our school, its workforce and our pupils is vital for the government in shaping the education system in the UK. Further details about statutory data sharing can be found in our privacy notices.

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 to our staff and pupils – for example, IT companies. 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 United Kingdom, we will do so in accordance with data protection law.

8.1. Sharing Safeguarding Data

In the event that the school deems it necessary to share data to protect a child, we will seek consent from the parent or legal guardian but only if it is appropriate to do so. Data protection law provides the school with a lawful framework to share data without the consent of the parent if there is a genuine concern for a childs health and wellbeing.

In addition, paragraph 119 of Keeping Children Safe in Education 2024 KCSIE 24) states that:

The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children.

In accordance with paragraphs 92 and 93 of KCSIE 24, our governing body and proprietors are aware that among other obligations, the Data Protection Act 2018, and the UK General Data Protection Regulation (UK GDPR) place duties on organisations and individuals to process personal information fairly and lawfully and to keep the information we hold safe and secure.

We will refer to the ICO guidance 'For Organisations' which includes information about our obligations and how to comply, including protecting personal information, and providing access to official information if data sharing is required to safeguard a pupil.

Please refer to our 'Safeguarding Policy' for further information.

9. Rights of Individuals

All individuals have rights with regards to their own (or their childs) personal data in certain circumstances. The school has implemented measures to support the rights of individuals where applicable.

9.1. Subject Access Requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with?
- How long the data will be stored for, or if this is not possible, the criteria used to determine this period
- 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

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

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

The school reserve the right to verify the identity of the individual making the request.

9.2. 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
- 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.

9.3. Recording Subject Access Requests

A record will be kept of all Subject Access Requests and logged on the SAR database. This SAR folder and database will be securely stored on site.

A file is to be created for each subject access request and in it should be the following information:-

- Copies of the correspondence between the Trust and the data subject, and between the school and any other parties.
- A record of any telephone conversation used to verify the identity of the data subject
- A record of the decisions and how the school came to those decisions
- Copies of the information sent to the data subject. For example, if the information was anonymised, keep a copy of the anonymised version that was sent to the data subject.

The file will be kept for one year and then securely destroyed.

When the request has been completed, the record of the request will be closed in the database.

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
- 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 United Kingdom
- 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.

10. Parental Requests to See the Educational Record

In addition to data protection rights, education law permits parents, or those with parental responsibility, the 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. Data protection will apply where necessary to the records provided.

11. CCTV

We use CCTV in various locations around the school site to ensure security. 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 Head of School.

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 photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

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
- For annual photographs of individual pupils and year groups made available for purchase by parents

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.

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

13. 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)
- Completing privacy impact assessments 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
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- 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

14. 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, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB 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 (see our IT 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)

15. 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.

The school will keep a record of any data destroyed.

16. 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:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium

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

17. 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.

18. Monitoring Arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed every 2years or sooner if any fundamental change in legislation occurs.

The policy will be reviewed 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.

Data protection breaches could be caused by a number of factors. Some examples are:

- Loss or theft of pupil, staff or Governors data and/ or equipment on which data is stored;
- The sharing of system passwords
- Inappropriate access controls allowing unauthorised use;
- Equipment Failure;
- Human Error;
- Unforeseen circumstances such as fire or flood;
- Hacking;
- 'Blagging' offences where information is obtained by deception.

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
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people

The DPO will alert the Headteacher and the chair of the 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
- Identify theft or fraud
- Financial loss
- Unauthorised reversal of pseudonymisation (for example, key-coding)
- Damage to reputation
- 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 in the designated, protected folder on each school's 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
- 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 72hours. 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
- 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 in the designated, protected folder on each school's system.

Review and Evaluation

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. A further review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

Once the initial aftermath of the breach is over, the DPO and Headteacher should fully review both the causes of the breach and the effectiveness of the response to it. It should be written and sent to

the next available School/Governing Board meeting for discussion. If there is the perception that this could be a continuing risk, the school's risk register is to be updated accordingly and an action plan must be drawn up to address the risk. This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

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 IT Manager 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: System Compliance

SIMS

Data	Pupil data – Addresses, Names, DOBs, Family contacts, Siblings, Medical Data, Meals, birth certificates, and other personal documents, passports Parent information's- Names, contact details, DOB, legal access. Staff information – Names, Addresses, contact details, next of kin, Medical issues, private documents, sickness, appraisals, employment.
Input	Admin Teams
Permission	General Privacy Notices
Used	Census – daily school management – emergencies
Deletion	DOB + 18 years
Third Party	Local Authority - Sims

Operoo

Data	Pupil data – Addresses, Names, DOBs, Family contacts, Siblings, Medical Data, Meals, birth certificates, and other personal documents, passports Parent information's- Names, contact details, DOB, legal access. Staff information – Names, Addresses, contact details, next of kin, Medical issues, private documents, sickness, appraisals, employment. E-Form management – leave of absence, policy documents
Input	Admin Teams
Permission	General Privacy Notices
Used	Daily school management – emergencies
Deletion	All data exported to relevant pupil/staff file and retained for correct length of time as per Records Management Policy
Third Party	Operoo

One Education HR & Clerking

Data	HR - Staff information – Names & addresses, Medical issues if required, private documents, sickness, appraisals, employment.

	Clerking – information provided as part of governing body reports
Input	SBM & SLT
Permission	General Privacy Notices
Used	Daily Management, Legal requirement
Deletion	In line with Records Management Policy
Third Party	One Education HR Team & Clerk to Governors

Staff files on computer and paper based

Data	Wide and varying material to monitor child progression – will include specific information to the role.
Input	Self-recorded by staff
Permission	Staff Privacy Notice
Used	Help with day-to-day management and school operations
Deletion	End of year deletion or port to next teacher
Third Party	Local Authority (HR & Payroll)

Website & Class DoJo

Data	Information held about the school and includes pictures and non-identifiable information.
Input	Senior Staff
Permission	General Privacy Notices & Online Safety Policy
Used	For people to find out about the school and what the class have been doing on a daily basis. Dojo can be used for outgoing and incoming communication.
Deletion	Yearly update and compliance check
Third Party	School Spider

CPOMs

Data	Child Protection monitoring, safeguarding and pastoral / welfare monitoring

Input	All staff can input – but access is limited to need to know.
Permission	Privacy Notice for Pupils / Parents
Used	Support children while in the school
Deletion	After the child reaches the age of 25
Third Party	CPOMS

Medical Tracker

Data	Pupil data – Names, DOBs, , Medical information, first aid Staff information – Names, DOBs, , Medical information, first aid
Input	Admin Teams & First Aiders
Permission	General Privacy Notices
Used	Daily school management – emergencies
Deletion	Current + 5 years unless relating to an accident at work which requires 12 years + retention or 25 years if relating to a major incident during a school trip or event.
Third Party	Medical Tracker

Juniper

Data	Allows for analysis and sharing of pupil progress and attainment data.
Input	Teachers
Permission	Privacy Notice for Pupils / Parents
Used	To monitor the progress of children's education
Deletion	Three years from current year
Third Party	O-Track

Bounce Together

Data	Allows for recording and analysis of pupil and staff surveys
Input	All staff & pupils
Permission	Privacy Notice for Pupils / Parents & staff
Used	To monitor the wellbeing of pupils and staff

Deletion	Operational use only
Third Party	Bounce Together

SENDIT

Data	SEN documentation and targets
Input	All staff can input but limited to need to know
Permission	Privacy Notice for Pupils / Parents
Used	Monitor SEN pupil progress in school
Deletion	After the child reaches the age of 25
Third Party	Impact Education

External Agency Support

Data	Data required for interventions and music tuition. Only necessary data is shared with each provider such as child name, year group, and current assessment level.
Input	School Staff & External Party
Permission	Privacy Notice for Pupils / Parents
Used	To monitor the progress of children's education
Deletion	If forms part of pupil record DOB + 18 or 25 years.
Third Party	Music Tutor, OT, SAL, Ed Psych

Visitor Management

Data	Records and stores details of visitors to the school, including name, times, who they are seeing, vehicle details and DBS checks
Input	Self-Recorded & Admin Team
Permission	Privacy Notice for Visitors
Used	To allow for management of visitors to the school.
Deletion	Self-Archiving
Third Party	InVentry

Pupil Assessment

Data	General pupil data plus assessment data
Input	Teachers
Permission	Privacy Notice for pupils/parents
Used	To monitor the progress of pupils in class through assessments
Deletion	No retention unless forming part of the pupil record.
Third Party Software Used:	FFT, GL Education, 3P Learning, Renaissance Learning, TES Testbase, Rising Stars, NFER, Mathletics, Language Links, Duolingo, Education City, Education Shed, Boardmaker, 2 Simple, Evidence Me, Spag.com, Pobble

CCTV

Data	Images of pupils, staff, visitors and members of the public
Input	Individuals recorded
Permission	No permission required; individuals informed by privacy notice, CCTV policy and signage on and around site
Used	Prevention & detection of crime and to protect the school's pupils, staff, visitors, community and also assets.
Deletion	Data kept for 30days then overwritten.
Third Party	PSN Monitoring