Roundwood
PRIMARY SCHOOL

# Data Protection Policy

| | | | |
|---|---|---|---|
| **Approved by:** | M Peters | **Date:** | Jan 26 |
| **Last reviewed on:** | Jan 26 | | |
| **Next review due by:** | Jan 2027 | | |

## 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 (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

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

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

## 3. Definitions

| Term | Definition |
|---|---|
| **Personal data** | Any information relating to an identified, or identifiable, individual.<br><br>This may include the individuals:<br>• Name (including initials)<br>• Identification number<br>• Location data<br>• Online identifier, such as a username<br><br>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:<br>• Racial or ethnic origin<br>• Political opinions<br>• Religious or philosophical beliefs<br>• Trade union membership |

| | |
|---|---|
| | • Genetics<br>• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes<br>• Health – physical or mental<br>• Sex life or sexual orientation |
| **Processing** | Anything done to personal data, such as collecting, recording, organizing, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing, or destroying.<br>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 means of processing personal data. |
| **Data processor** | A person or other body, other than an employee of the data controller, processes personal data on behalf of the data controller. |
| **Personal data breach** | A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. |

#### 4. The data controller

Our 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 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.

### 5.1 Governing board

The governing board is responsible for ensuring 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.

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

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

Our DPO is contactable on 01280 813066 at Roundwood Primary School or dpo.roundwood@gmail.com

### 5.3 Headteacher

The headteacher acts as the data controller's representative daily.

### 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 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
- If they need help with any contracts or sharing personal data with third parties

**6. Data protection principles**

The UKGDPR 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.

**7. Collecting personal data**

## 7.1 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 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 UKGDPR 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).

### 7.2 Limitation, minimisation and accuracy

We will only collect personal data for specific, explicit, and legitimate reasons. We will explain these reasons to 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.

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 retention schedule policy.

#### 8. Sharing personal data

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, if 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 respond to an emergency that affects any of our pupils or staff.

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

## 9. Subject access requests and other rights of individuals

### 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 isn't 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 should include:

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

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

### 9.2 Children and subject access requests

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

While younger children may be less likely to fully understand their rights, each request will be assessed on a case-by-case basis in line with ICO guidance. Most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the student. 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
- 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.

### 9.4 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 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.

## 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.

## 11. 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 noticeboards 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 child protection and safeguarding policy for more information on our use of photographs and videos.

### 12. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all 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 an elevated risk to rights and freedoms of individuals, and when introducing modern 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

## 13. 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:

- Data is securely stored and transferred on 2FA secured drives in password protected folders, using secure LA and DfE portals. Access levels are granted to staff where necessary. Emails are encrypted and accessed by 2FA.
- Papers containing confidential personal data are securely disposed of under the retention of the data table.
- 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
- 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)

## 14. Disposal of records

Personal data that is no longer needed will be disposed of securely in line with our Retention of Data Policy. 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 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.

## 15. Personal data breaches

The school will make all reasonable endeavors 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 (about 3 days). 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

## 16. 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 processes make it necessary.

## 17. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated, if necessary, when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed annually and shared with the full governing board.

## 20. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Child Protection & Safeguarding
- Acceptable Use of ICT

## 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
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will alert the head teacher 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
    - 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 later by the ICO or an individual affected by the breach. Documented decisions are stored on schools' computer systems.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 3hours (about 3 days). 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 possible 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 possible 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
    - 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 school's computer system
- The DPO and head teacher will meet to review what happened and how it can stop 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 breaches, 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.

***For example:***

- *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*
- *Details of pupil premium interventions for named children being published on the school website*
- *Non-anonymised pupil exam results or staff pay information being shared with governors*
- *A school laptop containing non-encrypted sensitive personal data being stolen or hacked*
- *The school's cashless payment provider being hacked and parents' financial details stolen*

**GDPR Data Retention Policy Roundwood Primary School**

| | |
|---|---|
| **Data Protection Officer (DPO) & Data Controller**<br><br>**It is recommended that the DPO is not a decision maker around the use of data i.e. headteacher or chair of governors. A person who might be suitable is a business manager, senior admin or governor**. | The school has a DPO and a DPO email address which is actively monitored.<br>Dpo.Roundwood@gmail.com<br>The school saves policies, data breeches and training logs on its 2FA secured GDPR drive. |
| **Clear Desk Policy & computers** | All staff are reminded regularly at staff meetings that their computers should not be left on and unattended at any time either at school or at home.<br>Sensitive personal data should be kept on 2FA drive. |

| | |
|---|---|
| **Staff Information Board Displays** | Personal data should not be displayed or accessible by pupils or parents.<br>Information is stored on the inside door of the teacher's cupboards in the classroom. Pupil medical information is on the staffroom noticeboards and covered by a front sheet and inside the door of the first aid cupboard. |
| **Assessment Data** | This is only shared outside school under statutory reasons or by agreement with DFE or LA. A request by a pupil or parent for their own data can be given out. There is a facility to report from Sims. There is no charge to the requestor**.** |
| **Governors** | Governors are bound by the school policy regarding data protection. Data should not be shared with third parties. Emails should only be shared with other governors and the staff . Data is shared on secure portal Governor hub. |
| **Timelines for keeping pupil data** | School will delete photos of pupils from secured devices and Secure server when pupil leaves school. Pupil data will be transferred to a new school or secondary school when the pupil leaves. |
| **A 1 Sims Data Base** | Pupil & staff information is stored in a secure SIMS database. Security and |

| | |
|---|---|
| | access to SIMS comply with the data protection policy. |
| **A2 Pupil File** | Digital records are retained on a secure Drive. When a pupil moves to a new school or moves up to secondary school, their files are transferred with them. |
| **A3 Admissions** | Information is stored on a secure drive then input into a secure SIMS database. Admissions data is stored on SIMS from admissions date. |
| **A4 N/A** | |
| **A5 Registers Attendance and Absence** | Attendance Information input into secure SIMS database Registers for SEND pupils are archived and kept until pupils 30th birthday, then records securely disposed of.<br>Records are transferred if the pupil leaves to go to another school.<br>Attendance records are kept for 3 years from the date of entry and then securely disposed of. |
| **A6 Behaviour Management** | Documents are kept by HT on secure 2FA drive or CPOMS and transferred to secondary or if pupil leaves to go to a new school. Documents are securely disposed of after the pupil leaves. |
| **A7 Behaviour Support** | Documents are kept by HT on secure 2FA drive or CPOMS and transferred to secondary or if pupil leaves to go to a |

| | |
|---|---|
| | new school. Documents are securely disposed of after the pupil leaves. |
| A8 **Achievement Management** | Monthly Marvellous Me information is received from teachers and displayed on board in school. This changes every month. |
| **Currcicular Records** | Retained on secure Drive for 1 year and disposed of securely. |
| **Records of Education Visits** | 10 years from the date of the visit.<br><br>If incidents on the visit, then records are retained, Inc. the permission slips, for all pupils and the incident report in the pupil record, or until the pupil reaches the age of 25. |
| A9 **Evolve** | Deputy Head teacher is Evolve coordinator and oversees information uploaded by teachers for trips. Records are securely deleted when pupils transition to secondary or if they leave to transfer to another school. |
| A10 **Clubs** | Paper copies of club choices are kept in the school office and shredded termly. Information is shared among teachers. Info on server is deleted annually |
| A11 **Free School Meals** | Spreadsheet of who is eligible is kept on secure server and shared with LA/ DfE. Information is kept until the pupil leaves school and is then securely disposed of. |
| A12 **School Meals** | Information is shared with authorised staff and hot meal providers. Data is securely disposed of annually. |

| | |
|---|---|
| **A13 Sims Staff** | Staff data is stored on Sims and remains on Sims for 6 years after the termination of their employment. Records are disposed of securely.<br><br>Staff HR records stored on the secure drive remain archived for 6 years after the termination of their employment. Records are disposed of securely.<br><br>Staff Pay Records are retained for 3 years from the end of the tax year they relate to. They are secured on the drive and shared with the LA through a secure portal. Records are disposed of securely. |
| **A14 Performance Management** | Digital copies of performance reviews carried out by HT and DH are securely stored on 2FA drive with secure access levels. |
| **A15 Staff Absences** | Are recorded in Sims for each staff member. Any medical information is also shared with insurance – if a claim is made. The information remains linked to the staff member in Sims |
| **A16 Staff Health Records** | Retained while the worker is employed in school. Securely disposed of after worker has left school.<br><br>Maternity records are retained for 3 years until the end of the tax year in which the maternity period ends. Records are securely disposed of. |
| **A17 Training** | Courses are recorded in sims linked to staff and are kept on G drive. |

| | |
|---|---|
| | Information such as names is shared with the agency running the course. |
| A18 **Recruitment** | Paper copies of applications are kept shortlisting and or deleted from server. Shortlisted applications are kept for 6 years. Information is kept on secure access restricted server. |
| A19 **Disciplinary and Allegations of child protection against a member of staff, including unfounded allegations** | Information is stored on a secure 2FA drive and is kept for 6 years. Data may be shared if required with LA, unions, and HR staff. Data is securely disposed of after 6 years.<br>For Allegations these are retained until staff retirement age or 10 years from the allegation, whichever is the latest.<br>Records are disposed of securely. |
| A 20 **FMS** | FMS is a secure portal for sharing transactions and salary payments by the school. Records are retained for 6 years and then securely disposed of.<br>Debtor's records, contracts and VAT records retained on secure school drive for 6 years from the end of the financial year. |
| A21 **School Fund** | Secure access to banking school fund by PIN. Data is shared with governors on Governor Hub. Documents retained for 6 years from the end of the financial year then securely disposed of. |

| | |
|---|---|
| A22 **Budget Tool** | Financial data is retained on a secure 2FA Drive and sent via a secure portal to LA and retained for 6 years, before being securely disposed of. |
| A23 **Pupil Premium** | PP Information is stored securely in Sims and on 2FA Drive. Data is deleted after 6 years. |
| A24 **Parent Mail/Pay** | Password protected portal that securely stores parent's bank payment details and email addresses for parent necessary parent school communication and payments. Information is securely stored and meets compliance requirements.<br>Information is securely disposed of by Parent Pay when the pupil leaves school.<br>Parent Pay Privacy notices available to parents. |
| A25 **Progress and Attainment Trackers** | Staff use this programmes to monitor progress and attainment. It is password protected, and information is securely disposed of when pupils leave. |
| A28 **Pupil Medical Information** | This is for the wellbeing of pupils and the information is shared with all staff and is stored in Sims. Paper copies are in a covered file on staffroom noticeboard and in lockable cupboards in the classroom. These are securely disposed of when the pupil leaves school. |
| A29 **Medicines** | The file contains information on medicine and how to administer it to students. The file is stored in the staffroom/office. Sheets are securely disposed of annually. |

| | |
|---|---|
| **A30 Single Central Record** | This is a safeguarding spreadsheet for staff, volunteers etc. Information is shared with the safeguarding governor, HT, and finance officer. It is stored on a 2FA drive with restricted access. Leavers are deleted from the SCR immediately.<br><br>Copies of DBS certificates are kept for a maximum of 6 months from the date of recruitment, and then securely disposed of. |
| **A31 Interventions** | Staff work with SEN children as needed. Information is linked to the SEN register; see below. |
| **A32 Special Educational Needs and disabilities, (SEND) Including SEND statements and accessibility plans.** | Records used for management of SEN plans and accessibility work, shared with SENDCO, SLT, LA and DfE. Information securely stored on SIMS and secure 2FA drive until pupils 30th birthday, when it is securely disposed of, unless the document is subject to legal hold. If the pupil leaves to go to another school, the records are transferred to that school. |
| **A33 Child Protection Records** | Separate CPOMS system used to securely store and share Child Protection Files. In line with Keeping Children Safe in Education.<br><br>Files are shared with LA, NHS, Staff, and external providers as approved. Access is password protected on 2FA server.<br><br>Information is retained until the child's 25th birthday. If the file relates to child sexual abuse retain until the child's 75th birthday. Records are disposed of securely. |

| | |
|---|---|
| | Child protection files are transferred separately from the main pupil file to any new school child attends. |
| **A34 Bucks Schools Team & Comtech** | Bucks Schools Team & Comtech have High level secure access to Schools SIMS and have permissions to account permits them to support calls and log on remotely to solve technical problems. |
| **A35 Inventory** | Visitors' books are kept in the reception area. Books are kept for 3 years and then shredded. |
| **A37 Accident Records** | A logbook is kept in the staff room and records all accidents to pupils, visitors, and staff. It is archived then securely disposed of 3 years from date of accident. |
| **A38 Governors File** | Information is stored on cloud-based password protected Governor Hub. Governors, HT, and finance officers have access to this site. Passwords are changed when there is a change in the governor. The Governor's reports are stored securely on the Governor Hub for 10 years and disposed of securely. |
| **A 40 Photos** | The school has a retention schedule for photos. When collecting consent for photographs to be used, the school specifies how they intend to retain the images and for how long. This statement will be included in the admission pack.<br>Permission for use of images is included in the admission pack. |

| | |
|---|---|
| | Photos of pupils for records and displays are taken with school iPad and are securely disposed of when pupils leave school. |
| A50 **B2B** | This data is backed up overnight and shared with the LA. SIMS and school have responsibility for information. |
| A51 **Website** | This provides the public with information regarding the school. The website is password protected and admin staff and teaching staff have access to upload information and delete it as required to keep the website up to date. |
| A52 | |
| A53 **Curriculum Sign ons** | Sign-Ons and access privileges are deleted when staff members leave the school, and new ones are allocated to new staff. |
| A54 **Correspondence** | Correspondence is securely stored on 2 FA drive which is password protected. It is deleted in line with the data retention period. |
| A55 **School Archive** | Archives are regularly inspected to ensure compliance with data retention schedules. |
| **School Vehicles** | Records retained for 6 years from date of disposal of vehicles. Records disposed of securely. |
| **Monitoring exposure to substances hazardous to health, inc asbestos** | Records retained for 5 years, then information disposed of securely. |

| | |
|---|---|
| **Maintenance Records** | Records retained for 6 years from end of financial year. Records disposed of securely. |
| **Fire Assessments** | Life of risk assessment plus 6 years. Records disposed of securely. |
| **Title Deeds** | 12 years from the end of the deed. Records disposed of securely. |
| **USB Sticks** | These are not safe and secure methods of storing pupil data. They are not allowed in school. |
| **School Privacy Notice** | Privacy Notices were updated in Jan 2025 and posted on the school website. Privacy notices for staff and pupils are in place. |
| **Who is responsible for PTA data? School or PTA?**<br>**The PTA is a separate group and responsible for their own data. Schools should not share personal data about pupils or staff with the PTA who do not have any specific legal right of access to this information.** | The PTA is a separate group and responsible for their own data. School will not share personal data around pupils or staff with the PTA who do not have any specific legal right of access to this information. |
| **Are Teachers allowed to take books home to mark? Laptops?** | Yes, as long as information is kept secure when not being used. Laptops should not be left in cars overnight, and access to laptops is by 2FA. |
| **Pupil files being sent to schools at end of school year.** | Files are delivered by hand or through the LA secure CTF portal. On occasion, files are sent by royal mail. |

| | |
|---|---|
| **Pupil Workbooks** | These should be given back to pupils at the end of their time in primary school and any that is not taken should be securely disposed of. |
| **AnyComms and Service portal** | AnyComms & Service Now is a LA secure encrypted portal for the transfer of data and information between the LA and the school. |
| **eMail** | Email is accessed by 2FA and provided by Microsoft 365. All emails are encrypted to the required compliance level.<br>Staff use email to correspond and send non-sensitive information to staff, LA, and other approved providers. |
| A 50 **School servers & laptops back up B2B** | Data is stored on in-house secure servers with restricted access and is backed up weekly. Laptops should not be left unattended in the classrooms and either locked securely in cupboards at the end of the day or taken home and secured safely. Access to school data on laptops is through 2FA and restricted password access. |
| **Third Parties using school data**<br>**Capita Sims- pupil & staff data base**<br>**Target Tracker – pupil assessment**<br>**Parent Mail+Pay – payments for trips, meals etc**<br>**Tapestry – Foundation Stage Learning** | The Privacy Notices & contract information are all stored in the GDPR file. These are being reviewed and updated by relevant companies. The data will provide information on what they do with the information, how they store it and how secure it is. They will also provide information on what they do with the data if the school does not renew a contract with them. Parent |

| | |
|---|---|
| | Mail+Pay no longer email bank account information, and customers can now access information online through their password protected account. |
| **What are definitions & levels of sensitive data** | Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or TU membership, processing of 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. Information relating to criminal convictions/history is not defined as 'sensitive personal data' but should only be used in ways defined by law (safeguarding/DBS etc.) |
| **A 35 Visitors Book** | Data collected is hidden and retained securely for 3 years. Data is securely disposed of. |
| • **'Right to be Forgotten'** The right to erasure is also known as 'the right to be forgotten.'<br>• The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.<br><br>In brief<br><br>When does the right to erasure apply?<br><br>The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal | |

| | |
|---|---|
| data erased and to prevent processing in specific circumstances:<br><br>• Where personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.<br>• When the individual withdraws consent.<br>• When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.<br>• The personal data was unlawfully processed (ie otherwise in breach of the GDPR).<br>• The personal data must be erased to comply with a legal obligation.<br>• The personal data is processed in relation to the offer of information society services to a child.<br><br>Under the GDPR, this right is not limited to processing that causes unwarranted and substantial damage or distress. However, if the processing does cause damage or distress, this is likely to make the case for erasure stronger.<br><br>There are some specific circumstances where the right to erasure does not apply, and you can refuse to deal with a request.<br><br>When can I refuse to comply with a request for erasure?<br><br>You can refuse to comply with a request for erasure where the personal data is processed for the following reasons:<br><br>• to exercise the right of freedom of expression and information;<br>• to comply with a legal obligation for the performance of a public interest task or exercise of official authority. | |

- for public health purposes in the public interest;
- archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- the exercise or defence of legal claims.

How does the right to erasure apply to children's personal data?

There are extra requirements when the request for erasure relates to children's personal data, reflecting the GDPR emphasis on the enhanced protection of such information, especially in online environments.

If you process the personal data of children, you should pay special attention to existing situations where a child has given consent to processing and they later request erasure of the data (regardless of age at the time of the request), especially on social networking sites and internet forums. This is because a child may not have been fully aware of the risks involved in the processing at the time of consent (Recital 65).

Do I have to tell other organisations about the erasure of personal data?

If you have disclosed the personal data in question to others, you must contact each recipient and inform them of the erasure of the personal data - unless this proves impossible or involves disproportionate effort. If asked to, you must also inform the individuals about these recipients.

| | |
|---|---|
| The GDPR reinforces the right to erasure by clarifying that organisations in the online environment who make personal data public should inform other organisations who process the personal data to erase links to, copies or replication of the personal data in question.<br><br>While this might be challenging, if you process personal information online, for example on social networks, forums, or websites, you must endeavor to comply with these requirements. As in the example below, there may be instances where organisations that process personal data may not be required to comply with this provision because an exemption applies.<br><br>**Example**<br><br>A search engine notifies a media publisher that it is delisting search results linking to a news report due to a request for erasure from an individual. If the article publication is protected by the freedom of expression exemption, the publisher is not required to erase the article. | |

| | |
|---|---|
| **The categories of school workforce information that we collect, process, hold and share include:** | We use school workforce data to: |

| | |
|---|---|
| • personal information (such as name, employee or teacher number, national insurance number)<br>• special categories of data including characteristics information such as gender, age, ethnic group<br>• contract information (such as start dates, hours worked, post, roles and salary information)<br>• work absence information (such as number of absences and reasons<br>• qualifications (and, where relevant, subjects taught | • enable the development of a comprehensive picture of the workforce and how it is deployed<br>• inform the development of recruitment and retention policies<br>• enable individuals to be paid |
| **The categories of pupil information that we collect, hold and share include:**<br>• Personal information (such as name, unique pupil number and address)<br>• Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)<br>• Attendance information (such as sessions attended, number of absences and absence reasons)<br>• Assessment information<br>• Relevant medical information<br>• Special educational needs information<br>• Exclusions<br>• Behaviour | We use the pupil data:<br>to support pupil learning<br>to monitor and report on pupil progress<br>to provide appropriate pastoral care<br>to assess the quality of our services<br>to comply with the law regarding data sharing |