Roundwood
PRIMARY SCHOOL

Data protection policy

Approved by:	**Date:**
Last reviewed on:	
Next review due by:	

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 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 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.

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. 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

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

5.2 Data protection officer

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

They will provide an annual report of their activities directly to the 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.

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

Our DPO is Turniton and is contactable via 01865 597620

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 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 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.

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 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 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).

7.2 Limitation, minimisation and accuracy

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

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

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

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, 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 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.

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.

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

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

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

See our 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 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

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:

- 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 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)

14. 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.

15. 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

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's 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 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
    - 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 on 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
    - 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
    - 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 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.

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 Policy Roundwood Primary School – Blue Highlights refer to IAR

Data Protection Officer (DPO) & Data Controller **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 appointed Turniton as DPO.
Clear Desk Policy & computers **Keeping desks clear and computer screens locked down when not in use would minimise the risk of a data breach through loss of data or inappropriate access by pupils/parents or visitors**	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. Sensitive personal data should be kept in a secure location. All staff files containing personal data are in locked cupboards and cabinets in the office at the Gawcott site.
Staff Information Board Displays	Personal data should not be on display or accessible by pupils or parents. Information is stored on the inside door of teacher's cupboards in classroonm. Pupil medical information is on the staffroom noticeboards and covered by a front sheet.
Assessment Data **It is suggested that this is only shared outside school if under a statutory reason or by agreement with DFE or BCC. 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.**	Staff will be reminded regularly at staff meetings.
BC courier service	This is being reviewed but Buckinghamshire Council anticipate this will continue to remain secure

Governors	Governors are bound by the school policy regarding data protection. Data should not be shared with third parties. E:mails should only be shared with other governors and the staff governors.
Timelines for keeping pupil data	School will delete photos of pupils from laptops and server when pupil leaves school. Pupil data will be deleted once pupil leaves school. Sims Data kept till process to delete is resolved. SEN information is stored until the pupil reaches the age of 25 years.
A 1 **Sims Data Base**	Pupil & staff information is stored on password protected server, networked to 3 admin and headteacher. Programme is password protected and roles and responsibilities allocated. Information is on sims as no way to delete pupil records
A2 **Pupil File**	Records are kept in lockable cupboard in lockable office and when pupil leaves file is sent to new school or shredded.
A3 **Admissions**	Information is stored in lockable admin offices before being input into sims. Information remains on Sims
A4 N/A	
A5 **Registers**	Paper copy of registers are kept in office and collected twice a day by pupils and completed by teachers. Information is then input into Sims. Registers are archived and kept for 6 years
A6 **Behaviour Management**	A behaviour log book is kept in staff room. Kept for a year and then archived
A7 **Behaviour Support**	Paper documents are kept by HT in her office and kept for a year then archived for 6 years
A8 **Achievement Management**	Monthly Marvel information is received from teachers and displayed on board in school this is changed every month.
A9 **Evolve**	Deputy Headteacher is Evolve co-ordinator and oversees information

	uploaded by teachers for trips. Records remain on Evolve until manager of Evolve deletes them
A10 **Clubs**	Paper copies of club choices are kept in school office and shredded termly. Information is shared amongst teachers. Info on server is deleted annually
A11 **Free School Meals**	Spreadsheet of who is eligible is kept on server and shared with LA who do a check list. Information is kept until pupil leaves school and is then deleted from server
A12 **School Meals**	Information is shared with Admin staff, hot meal provider and ParentMail+Pay. Information is deleted from server annually and ParentMail+Pay
A13 **Sims Staff**	Staff data is stored on Sims and remains on Sims after the person has left the school.
A14 **Performance Management**	Paper copies of performance reviews carried out by HT and DH are given to finance officer who inputs information onto Sims
A15 **Staff Absences**	Are recorded in Sims for each staff member. Information is also input through the Eforms portal. Any medical information is also shared with insurance company if a claim is made. The information remains linked to the staff member in Sims
A16 **Sickness Claims**	See above
A17 **Training**	Courses are recorded in sims linked to staff and is kept on sims. Information such as names are shared with the agency running the course
A18 **Recruitment**	Paper copies of applications are kept until shortlisting and then shredded or deleted from server. Shortlisted applications are kept for 6 years. Information is kept in lockable office
A19 **Disciplinary**	Information is kept in HT lockable office in lockable cabinet and kept for 6 years. Information is shared with Unions and LA

A 20 **FMS**	The school keeps copies of suppliers' privacy notices. This shows how they process information and their GDPR compliance Personnel links into FMS for salary commitments FMS is password protected and roles and responsibilities restricts access.
A21 **School Fund**	Spreadsheet is kept on password protected server and networked to admin laptop. Information is given annually to auditor and presented to governors. Information is kept for 6 years
A22 **Budget Tool**	Budget spreadsheet is password protected and kept for 6 years. Spreadsheet is shared with governors, HT and LA finance team
A23 **Pupil Premium**	This is for monitoring funding for FSM & LAC funded children. The funding is to support attainment and financial support for resources for pupils. Information is stored in Sims and on spreadsheet on admin server . Spreadsheet is deleted after 6 years
A24 **Parent Pay**	Parents can pay for trips, meals etc using programme. It is password protected and holds bank payment details. Admin staff can access to monitor payment and reconcile with school bank account. Information is deleted by ParentPay when pupil leaves school. Parent Pay Privacy notice and statement are filed in school office
A25 **Target Tracker**	Staff use this programme to monitor progress and attainment. It is password protected and information is archived when pupils leave. Privacy Notice & statement are filed in school office
A28 **Pupil Medical Information**	This is for well being of pupil and 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 deleted when pupil leaves school. Information remains with pupil on Sims

A29 **Medicines**	File contains information on medicine and how to administer it to pupil. File is stored in staffroom/office. Sheets are shredded annually.
A30 **Single Central Record**	This is a safeguarding spreadsheet for staff, volunteers etc. Information is shared with safeguarding governor, HT and finance officer. It is stored on g drive on main server which is password protected. Information is deleted when person is no longer in contact with school.
A31 **Interventions**	Staff work with SEN children on an as needed basis. Information is linked to SEN register see below.
A32 **SEN Register**	This is used for management of SEN children and information is shared with staff and SEND co-ordinator. Information remains linked to pupil on Sims. Folders are in locked cupboard. Paper information on pupil remains until they reach the age of 25 when it is shredded.
A33 **Child Protection Folder**	The folder is used for safeguarding children and is kept in a lockable cupboard in HT 's lockable office. Information is shared with staff and outside agencies as required. Information is kept for 6 years
A34 **Bucks IT Schools Team & Compubits**	Bucks IT Schools Team & Compubits. High level account permits them to see support call and log on remotely to solve technical problems.
A35 **Inventory**	Visitors book is kept in reception. Books are kept for 3 years and then shredded.
A37 **Accident Log**	Log book is kept in staff room and records all accidents to pupils, visitors and staff. It is archived then shredded after 6 years.
A38 **Governors File**	Information is stored on cloud based password protected Governor Hub. Governors, HT and finance officer have access. Passwords are changed when there is a change in governor.
A 40 **Photos**	The school has a retention schedule for the use of 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. Permission for use of images is included in the admission pack. Teachers who take photos of children on their mobile phones must transfer them to their laptops , must then delete images from their phones
A50 **B2B**	This data is required by LA and is extracted from Sims. This runs overnight. LA has responsibility of information.
A51 **Website**	This provides the public with information regarding the school. The website is password protected and admin staff, teaching staff have access to upload information and delete as required to keep website up to date.
A52	
A53 **Curriculum Sign ons**	School is looking to have curriculum signons for cloud based sharing of folders with teachers. Sign ons will be deleted when staff member leaves the school and new ones allocated to new staff.
A54 **Correspondence**	Letters are stored on G drive which is password protected. They are deleted after 3 years from g drive.
A55 **School Archive**	SEN information is archived until pupil reaches age of 25 years then shredded.
USB Sticks	These are not a safe and secure method of storing pupil data. School will look into the secure Office 365 service provided by County to store pupil data in the Cloud. This data can only be accessed by users authorised by the school admin team.
School Privacy Notice	Privacy Notice was updated in May and posted on school website. Privacy notices for staff and pupils are in place.

Who is responsible for PTA data? School or PTA? **The PTA is a separate group and responsible for their own data. Schools should not share personal data around pupils or staff with the PTA who do not have any specific legal right of access to this information. School governors are different and act on behalf of the school and would be bound by the schools' policies and governance requirements (confidentiality etc)**	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. School governors are different and act on behalf of the school and would be bound by the schools' policies and governance requirements (confidentiality etc)
Are Teachers allowed to take books home to mark? Laptops?	Yes as long as information is kept secure when not being used. This information should not be left in cars overnight. This also applies to laptops
Pupil files being sent to schools at end of school year.	Post should be delivered correctly and to the right person. Files are delivered by hand where possible into the correct school offices at the end of year. On occasion files are sent by royal mail.
Pupil Workbooks	These should be given back to pupils and any that are not taken should be destroyed. The school needs to define a time for when the workbooks need to be destroyed after the pupil has left the school
BC eMail How secure is the system?	AnyComms is encrypted to the required compliance level. Staff & Parents have been sent a link to opt into e:mail. New parents are asked permission to send emails when they join school.
A 50 School serv ers & laptops back up B2B	Data is stored off site by overnight back up. The school buys this service through Buckinghamshire Council. 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.

Third Parties using school data **Capita Sims- pupil & staff data base** **Teacher Absence** **Target Tracker – pupil assessment** **Parent Mail+Pay – payments for trips, meals etc** **Tapestry – Foundation Stage Learning** **Lloyds Bank**	The Privacy Notices & contract information are all stored in the GDPR file. These are being reviewed and updated by the 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 e:mail bank account information and customers can now access information on line 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 are not defined as 'sensitive personal data' but should only be used in ways defined by law (safeguarding/DBS etc)	School must be aware of these definitions
A 35 Visitors Book	A GDPR compliant visitor book has been sourced.
• **'Right to be Forgotten'** The right to erasure is also known as 'the right to be forgotten'. • 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. In brief	

When does the right to erasure apply?

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:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (ie otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

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.

There are some specific circumstances where the right to erasure does not apply and you can refuse to deal with a request.

When can I refuse to comply with a request for erasure?

You can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

- to exercise the right of freedom of expression and information;

• 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. While this might be challenging, if you process personal information online, for example on social networks, forums or websites, you must endeavour to comply with these requirements. As in the example below, there may be instances where organisations that process the personal data may not be required to comply with this provision because an exemption applies. **Example** A search engine notifies a media publisher that it is delisting search results linking to a news report as a result of a request for erasure from an individual. If the publication of the article is protected by the freedom of expression exemption, then the publisher is not required to erase the article.	

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