Rosehill Infant and Nursery School

Data Protection Policy

Last updated: 4th December 2025

Review date: January 2027

Signed by:

	Headteacher	Date:	
	Chair of governors	Date:	

Data Protection Policy

Rosehill Infant & Nursery School is committed to working effectively to provide a secure environment to protect data that we hold and store. Whilst there is a statutory duty that is important, the fact that we store data about individuals means that we are responsible for your data, and we take that very seriously. This policy, and the Privacy Notices, set out how we look after and use data.

Our school is responsible for the day-to-day management of data that is held about pupils, staff, parents, carers and other individuals in connection with that school.

Where we use the phrase 'we' that refers to the school.

What is the General Data Protection Regulation (UK GDPR)?

This is a European Directive that was brought into UK law with an updated Data Protection Act 2018 (DPA) in May 2018. It was brought into line with changes to the UK leaving the EU on 31 December 2020.

The UK GDPR and DPA 2018 exist to look after individuals' data. It is a series of safeguards for every individual. Information about individuals needs to be treated with respect and be secure.

The UK GDPR exists to protect individual rights in an increasingly digital world.

Who does it apply to?

Everyone, including schools. As 'Public Bodies' schools and trusts have more obligations than some small businesses. It is mandatory to comply with the UK GDPR and provisions in the Data Protection Act 2018.

We want to make sure information about pupils, parents, staff and volunteers is kept secure and within the law.

What is personal data?

Any information that relates to a living person that identifies them. This can be by name, address, or phone number for example. It also relates to details about that person, which can include opinions.

Some data is considered to be more sensitive, and therefore more important to protect. This is information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sex life and sexual orientation, genetic data, and biometric data where processed to uniquely identify a person.

Schools often collect sensitive data for DfE and LA requirements and of course pupil data may contain information about safeguarding, SEN or health needs. Information about other family members may also be on the school file.

Privacy Notices that explain how data about specific groups or activities is used and stored are also available on our school website.

What are the key principles of the UK GDPR?

1. Lawfulness, transparency and fairness

Schools must have a legitimate reason to hold the data, we explain this in the Privacy Notices. We often ask for consent to use data about a pupil for a particular purpose. If you wish to withdraw consent, we have a form to complete to allow us to process your request. There are times when you cannot withdraw consent as explained in 'Data Subjects' Rights'.

2. Collect data for a specific purpose and use it for that purpose

Data cannot be used for a purpose that it was not originally collected for, or where notice has not been given about how data may be used after collection.

3. Limited collection

Data Controllers should only collect the minimum amount of data needed for a particular task or reason. If there is a breach or a hack only limited information can be lost.

4. Accuracy

Data collected should be accurate, and steps should be taken to check and confirm accuracy. This is done when pupils join the school and is reviewed on an annual basis.

If a Data Subject feels that the information held is inaccurate, should no longer be held by the Controller or should not be held by the Controller in any event, a dispute resolution process and complaint process can be accessed, using the suitable forms. Initially an approach should be made directly to the school.

5. Retention

A retention policy is in place that governs how long records are held for.

6. Security

We have processes in place to keep data safe. That might be paper files, electronic records or other information. Paper files that contain sensitive information are kept in a lock cabinet in a locked room. Electronic files are kept on the school's server and if necessary password protected. Please see information security policy, which can be found on our website Rosehill Infant and Nursery School - Policies

Who is a 'data subject'?

An individual whose details we keep on file. Some details are more sensitive than others. The UK GDPR sets out collection of details such as health conditions and ethnicity which are more sensitive than names and phone numbers.

Data subjects' rights

Individuals have a right:

- to be informed
- of access to data stored about them or their children
- to rectification if there is an error on the data stored
- to erasure if there is no longer a need for school to keep the data
- to restrict processing, i.e. to limit what is done with their data
- to object to data being shared or collected

There are other rights that relate to automated decision making and data portability that are not directly relevant in schools.

Data subjects' rights are also subject to child protection and safeguarding concerns and sharing information for the prevention and detection of crime. Schools also have legal and contractual obligations to share information with organisations such as the Department for Education, Social Care, the Local Authority and HMRC amongst others. In some cases, these obligations override individual rights.

These 'Data Subject's Rights' are set out in more detail in the document 'My Rights – A Guide for Data Subjects'.

Subject Access Requests (SAR)

You can ask for copies of information that we hold about you or a pupil (who you have parental responsibility for). This SAR process is set out separately. You should complete the form, and you may need to provide identification evidence for us to process the request.

We have to provide the information within a month, but this can be extended if the request is complicated, or the data cannot be accessed.

When we receive a request, we may ask you to be more specific about the information that you require. This is to refine any queries to make sure you access what you need, rather than sometimes getting a lot of information that may not be relevant to your query.

In accordance with the Data (Use and Access) Act 2025, we are required to conduct searches that are reasonable and proportionate when responding to a SAR. If a request results in a substantial volume of data deemed to be unreasonable and disproportionate, we will notify you and offer an opportunity to refine the scope of your request. This allows you to specify the information you are seeking, enabling us to carry out a targeted search and provide the most relevant data.

In some cases, we cannot share all information we hold on file if there are contractual, legal or regulatory reasons.

We cannot release information provided by a third party without their consent, or in some cases you may be better to approach them directly, e.g. school nurses who are employed by the NHS.

We will supply the information by paper or electronic form.

If you wish to complain about the process, please see Appendix 1 within our Complaints Policy and later information in this DPA policy.

Who is a 'data controller'?

The school is the data controller and have ultimate responsibility for how the school manages data. The school will delegate this to data processors to act on the school's behalf.

The data controller can also have contracts and agreements in place with outside agencies who are data processors.

As the Data Controller, individuals process data on behalf of the organisation. This can be a member of staff, possibly a governor or trustee, a consultant or temporary employee.

Who is a 'data processor'?

This is a person or organisation that uses, collects, accesses, or amends the data that the controller has collected or authorised to be collected.

Data controllers must make sure that data processors are as careful about the data as the controller themselves. The UK GDPR places additional obligations on organisations to make sure that data controllers require contractual agreements to ensure that this is the case.

Processing data

The school must have a reason to process the data about an individual. Our Privacy Notices set out how we use data. The UK GDPR as amended by the Data (Use and Access) Act (DUAA) 2025 has seven conditions for lawful processing and any time we process data relating to an individual it is within one of those conditions.

If there is a data breach, we have a separate procedure to follow to take immediate action to remedy the situation as quickly as possible.

The legal basis and authority for collecting and processing data in school are:

- consent obtained from the data subject or their parent/carer
- performance of a contract where the data subject is a party
- compliance with a legal obligation
- to protect the vital interests of the data subject or other associated person
- to carry out the processing that is in the public interest and/or official authority
- it is necessary for the legitimate interests of the data controller or third party
- in accordance with national law
- to safeguard vulnerable individuals, crime prevention, and respond to emergencies.

In addition, any special categories of personal data are processed on the grounds of:

- explicit consent from the data subject or about their child
- necessary to comply with employment rights or obligations
- protection of the vital interests of the data subject or associated person
- being necessary to comply with the legitimate activities of the school
- existing personal data that has been made public by the data subject and is no longer confidential
- bringing or defending legal claims
- safeguarding
- national laws in terms of processing genetic, biometric or health data

Processing data is recorded within the school systems.

Data sharing

Data sharing is done within the limits set by the UK GDPR. Guidance from the Department for Education (DfE), health, the police, local authorities and other specialist organisations may be used to determine whether data is shared.

The basis for sharing or not sharing data is recorded in school.

Breaches & non-compliance

If there is non-compliance with the policy or processes, or there is a DPA breach as described within the UK GDPR and DPA 2018 then the guidance set out in the Breach & Non-compliance Procedure and Process needs to be followed.

Protecting data and maintaining Data Subjects' Rights is the purpose of this policy and associated procedures.

The Date Breach & Non-Compliance Procedures can be found at the end of this policy on apendix 1

Consent

As school, where required, we will seek consent from staff, volunteers, young people, parents and carers to collect and process their data. We will be clear about our reasons for requesting the data and how we will use it. There are contractual, statutory and regulatory occasions when consent is not required.

Consent is defined by the UK GDPR as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

We may seek consent from young people also, and this will be dependent on the child and the reason for processing.

This will largely be managed in school.

Consent and renewal

On the school websites we have 'Privacy Notices' that explain how data is collected and used. It is important to read those notices as it explains how data is used in detail. Please go to Rosehill Infant and Nursery School - Data Protection and Financial Information

Obtaining clear consent, where required, and ensuring that the consent remains in place is important for school. We also want to ensure the accuracy of that information.

For pupils and parents/carers

On joining the school you will be asked to complete a form giving next of kin details, emergency contact and other essential information. We will also ask you to give consent to use the information for other in-school purposes, as set out on the consent form.

It is important to inform school if details or your decision about consent changes. A form is available. This is the obligation of each individual to notify the school of changes.

Pupil consent procedure

Where processing relates to a child under 13 years old, school will obtain the consent from a person who has parental responsibility for the child as required.

Pupils may be asked to give consent or to be consulted about how their data is obtained, shared and used in certain situations.

Withdrawal of consent

Consent can be withdrawn, subject to contractual, statutory or regulatory constraints. Where more than one person has the ability to provide or withdraw consent the school will consider each situation on the merits and within the principles of UK GDPR and also child welfare, protection and safeguarding principles.

Please complete the appropriate form obtained from the reception office.

Data Protection Officer

We have a Data Protection Officer (DPO) whose role is to:

- inform and advise the controller or the processor and the employees who carry out processing of their obligations under the UK GDPR
- monitor compliance with the UK GDPR and DPA
- provide advice where requested about the data protection impact assessment and monitor its performance
- be the point of contact for Data Subjects if there are concerns about data protection
- cooperate with the supervisory authority and manage the breach procedure
- advise about training and CPD for the UK GDPR

Our DPO is John Walker whose contact details are below.

Address: The Brutus Centre, Station Road, Totnes, Devon TQ9 5RW

Email: info@phplaw.co.uk

Physical security

As a school we are obliged to have appropriate security measures in place.

In the school, every secure area has individuals who are responsible for ensuring that the space is securely maintained and controlled if unoccupied, i.e. locked. Offices and cupboards that contain personal data should be secured if the processor is not present.

The Head teacher is responsible for authorising access to secure areas.

All staff, contractors and third parties who have control over lockable areas must take due care to prevent data breaches.

All sites and locations need to have the suitable security and review measures in place.

Secure disposal

When disposal of items is necessary a suitable process must be used. This is to secure the data, to provide a process that does not enable data to be shared in error, by malicious or criminal intent.

These processes, when undertaken by a third party are subject to contractual conditions to ensure UK GDPR and DPA compliance.

Complaints & the Information Commissioner Office (ICO)

In accordance with requirements set out by DUAA 2025, the school has established a dedicated complaint procedure for data protection matters. Please see our Complaint Policy, Appendix 1.

There is a right to complain if you feel that data has been shared without consent or lawful authority.

You can complain if you have asked to us to erase, rectify, or not process data and we have not agreed to your request.

We will always try to resolve issues on an informal basis, and then through a formal procedure. Please complete our dedicated form, and we will contact you with more details about the timescale and process.

In the UK it is the ICO who has responsibility for safeguarding and enforcing the DPA obligations.

Email: casework@ico.org.uk

Helpline: 0303 123 1113

Website: www.ico.org.uk

Review

A review of the effectiveness of UK GDPR compliance and processes will be conducted by the DPO every 12/24 months.

Appendix 1

Data Protection – breach and non-compliance procedure

Breach management guidance

All staff, governors and trustees must be aware of what to do in the event of a DPA/UK GDPR breach. The 'Data Breach Flowchart' outlines the process.

Most breaches, aside from cyber-criminal attacks, occur as a result of human error. They are not

malicious in origin and if quickly reported are often manageable.

Everyone needs to understand that if a breach occurs it must be swiftly reported so that risks to the data subjects are minimized and well managed.

What is a breach?

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

Examples of breaches are:

- information being posted to an incorrect address which results in an unintended recipient reading the information
- loss of mobile or portable device, unencrypted mobile phone, USB memory stick or similar
- sending an email containing personal data to the wrong person
- dropping or leaving documents containing personal data in a public place
- personal data being left unattended at a printer enabling unauthorised persons to read that information
- not securing documents containing personal data (at home or work) when left unattended
- anything that enables an unauthorised individual access to school buildings or computer systems
- discussing personal data with someone not entitled to it, either by phone or in person. How can you be sure they are entitled to that information?
- deliberately accessing, or attempting to access or use personal data beyond the requirements of an individual's job role e.g. for personal, commercial or political use. This action may constitute a criminal offence under the Computer Misuse Act as well as the Data Protection Act.
- opening a malicious email attachment or clicking on a link from an external or unfamiliar source, which leads to school's equipment (and subsequently its records) being subjected to a virus or malicious attack which results in unauthorised access to, loss, destruction or damage to personal data

What staff and governors should do?

Being open about the possible breach and explaining what has been lost or potentially accessed is an important element of working with the ICO and to mitigate the impact. Covering up a breach is never acceptable and may be a criminal, civil or disciplinary matter.

Report the breach to the data controller, Data Protection Compliance Manager and DPO as soon as possible, this is essential.

How is the breach managed?

The breach notification form will be completed and the breach registered on the Go-GDPR portal.

Advice will be sought from the Data Protection Officer as required. A plan to effectively manage the breach, who to inform and how to proceed will be put in place.

If the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach notification to those people will be done in a co-ordinated manner with support from the DPO.

Actions and changes to procedures, additional training or other measures may be required to be implemented and reviewed.

The breach report will be within 72 hours of becoming aware of the breach to the Information Commissioner if it is serious.

It may not be possible to investigate the breach fully within the 72-hour timeframe. Information about further investigations will be shared with the ICO with support from the DPO.

What happens to the people whose data has been breached?

For every breach the school will consider notification to the data subject or subjects as part of the process. If the breach is likely to be high risk they will be notified as soon as possible and kept informed of actions and outcomes.

The breach and process will be described in clear and plain language.

If the breach affects a high volume of data subjects and personal data records, the most effective form of notification will be used.

Advice may be taken from the ICO about how to manage communication with data subjects if appropriate.

Evidence Collection

It may be necessary to collect information about how an information security breach or unauthorised release of data occurred. This evidence gathering process may be used as an internal process (which can include disciplinary proceedings), it may be a source of information for the ICO, it could also be used within criminal or civil proceedings.

This process will be conducted by a suitable member of school staff, which may be the Data Management Compliance Officer or Data Protection Officer but will be determined depending on the nature of the breach.

Guidance may be required from external legal providers and police may be involved to determine the best way to secure evidence.

A record of what evidence has been gathered, stored and secured must be available as a separate log. Files and hardware must be securely stored, possibly in a designated offsite facility.

What happens next?

The impact of a serious breach will need to be assessed. It may be necessary to change some processes and procedures.

Additional training may be required. IT protocols may need to be reviewed.

The school will work with the Data Protection Officer to ensure that any changes are made to protect and secure information and to learn from any breaches.