

St James the Less RC Primary School

Data Protection Policy

The following policy relates to all St James the Less RC Primary School employees (including voluntary, temporary, contract and seconded employees), who capture, create, store, use, share and dispose of information on behalf of St James the Less School.

These persons shall be referred to as 'Users' throughout the rest of this policy.

St James the Less RC Primary School shall be referred to as 'the school' or 'we' throughout the rest of this policy.

The following policy relates to all electronic and paper-based information.

Statement of Commitment

In order to undertake our statutory obligations effectively, deliver services and meet customer requirements, the school needs to collect, use and retain information, much of which is personal, sensitive or confidential.

Such information may be about:

- Pupils.
- Parents and Guardians.
- Governors.
- Employees or their families.
- Members of the public.
- Business partners.
- Local authorities or public bodies.

We regard the lawful and correct treatment of personal data by the school as very important to maintain the confidence of our stakeholders and to operate successfully.

To this end, the school will ensure compliance, in all its functions, with the Data Protection Act (DPA) 1998, the General Data Protection Regulation (GDPR) and the new Data Protection Act (DPA) 2018, and with other relevant legislation.

Data Protection Principles

The Principles of DPA and GDPR state that personal information must be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals; the lawful basis can be:
 - Consent of a data subject

- Processing is necessary for the performance of a contract with the data subject
- Processing is necessary for compliance with a legal obligation (e.g. The Education Act 1996, School Standards and Framework Act 1998, Education Act 2002, Children and Families Act 2014)
- Processing is necessary to protect the vital interests of the data subject or another person (e.g. life or death)
- Processing is necessary for the performance of a task carried out in the public interest

The lawful basis for sensitive personal data (racial, political, religious, trade union, genetic, health, sex life, criminal convictions or offences) is:

- Explicit consent of the data subject
- Processing is necessary for carrying out obligations under employment, social security or social protection law
- Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members and provided there is no disclosure to a third party without consent
- Processing relates to personal data manifestly made public by the data subject
- Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
- Processing is necessary for reasons of substantial public interest
- Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services
- Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices

- Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
 3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
 4. Accurate and, where necessary, kept up to date
 5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
 6. Processed in a manner that ensures appropriate security of the personal data against unauthorised processing, accidental loss, destruction or damage, using appropriate technical or organisational measures.

Compliance with the Data Protection Principles and Data Protection Legislation

In order to comply with these principles and meet all data protection obligations as stipulated in data protection legislation, the school will:

- Raise awareness of data protection across the school.
- Offer data protection training to all employees and governors.
- Create a data protection policy for the school that is updated annually.
- Complete a personal data processing audit, which lists the following:
 - Name of the personal data set.
 - Purpose for processing this personal data set.
 - Who the data set is shared with.
 - Is the data transferred to another country.
 - How long do you keep the personal data set (retention).
 - The technical and organisational security measures to protect the personal data set.
 - The legal basis for processing as described above (1).
 - If consent is the legal basis for processing, details of the evidence of this consent.
- Put any risks found from the personal data processing audit process into a risk register.
- Review the school's consent forms so they meet the higher standards of GDPR, create an audit trail showing evidence of consent.
- Under 13's can never themselves consent to the processing of their personal data in relation to online services, this rule is subject to certain exceptions such as counselling services.
- Register with the Information Commissioners Officer as a data controller.

- Appoint a data protection officer who will monitor compliance with the GDPR and other data protection laws.
- Create a privacy notice that will let individuals know who we are, why we are processing their data and if we share their data.
- Create a system to allow data subjects to exercise their rights:
 - Right to be informed via a privacy notice.
 - Right of access via a subject access request within 1 month.
 - Right of rectification to incorrect data within 1 month.
 - Right to erasure unless there is a legal reason for processing their data.
 - Right to restrict processing to the bare minimum.
 - Right to data portability to receive their data in the format they request.
 - Right to object to personal data being used for profiling, direct marketing or research purposes.
 - Rights in relation to automated decision making and profiling.
- Amend any business contracts with suppliers to ensure that they will conform to new data protection legislation.
- Implement technical and organisational controls to keep personal data secure.
- Use Privacy Impact Assessments to assess the privacy aspects of any projects or systems processing personal data.
- Ensure an adequate level of protection for any personal data processed by others on behalf of the school that is transferred outside the European Economic Area.
- Investigate all information security breaches, and if reportable, report to the Information Commissioners Office within 72 hours.
- Undertake data quality checks to ensure personal data is accurate and up to date.
- Demonstrate our compliance in an accountable manner through audits, spot checks, accreditations and performance checks.
- Support the pseudonymisation and encryption of personal data.

Rights of the Individual

The list of rights that a data subject (person who the data is about) can exercise has been widened by Section 2 of the GDPR:

- The right to be informed; via privacy notices.
- The right of access; via subject access requests (SARS), the timescale for response has been reduced from 40 calendar days to one calendar month. SARS must be free of charge, charges can only be made for further copies or where requests for information are unfounded or excessive.
- The right of rectification; inaccurate or incomplete data must be rectified within one month.
- The right to erasure; individuals have a right to have their personal data erased and to prevent processing unless we have a legal obligation to do so.
- The right to restrict processing; individuals have the right to suppress processing. We can retain just enough information about the individual to ensure that the restriction is respected in future.

- The right to data portability; we need to provide individuals with their personal data in a structured, commonly used, machine readable form when asked.
- The right to object; individuals can object to their personal data being used for profiling, direct marketing or research purposes.
- Rights in relation to automated decision making and profiling; GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.

The school will ensure that these rights will be exercised.

Contact

Contact the Data Protection Officer by:

Email: office@st-jamesless.lancs.sch.uk

Phone: 01706 216190

Post: Unity Way, Rawtenstall, Lancashire BB4 8SU

Version Control

Named Owner:	School Office Manager – Data Protection Officer
Version Number:	1.00
Date Of DPO:	
Most recent review:	Spring 2024

GDPR Statement – Website St James the Less RC Primary School

DATA PROTECTION OFFICER (DPO) CONTACT DETAILS The Data Protection Officer is responsible for overseeing data protection within the School so if you do have any questions in this regard, please do contact them on the information below:-

Data Protection Officer: Office Manager – A Connaghan
Company: St James the Less RC Primary School, Rawtenstall
Address: Unity Way, Rawtenstall, BB4 8SU
Email: office@st-jamesless.lancs.sch.uk
Telephone: 01706 216190

St James the Less RC Primary School strives to meet the standards, as set out in the GDPR and the Data Protection Act of 2018.

Data Protection Act 2018: How we use pupil information

General Data Protection Regulations (GDPR)

Who do we share pupil's information with?

We routinely share pupil information with:

- Schools or colleges that the pupils attend after leaving us
- Our local authority and their commissioned providers of local authority services
- The Department of Education (DfE)

Storing pupil Information

At St James the Less we keep information about children that attend this school on our computer systems and in hardcopy format (paper).

We hold your child's education records securely. Any essential records on an individual child follow them through their education establishments. St James the Less holds a record of the schools each child has moved to.

There are strict controls on who can see information about pupils. The school protects all data and will pay particular attention to the security of especially sensitive data. Parents / carers will be asked for their consent for the school to process some specific data (such as photographs).

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the School Census and Early Years' Census.

Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013. To find out more about the pupil information we share with the Department of Education, for the purpose of data collections, go to

<https://www.gov.uk/guidance/apply-for-department-for-education-dfe-personal-data>

The Department of Education may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- Conducting research or analysis
- Producing statistics
- Providing information, advice or guidance

The Department of Education has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether the DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- Who is requesting the data
- The purpose for which it is required
- The level and sensitivity of data requested and
- The arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the Department of Education's data sharing process, please visit

<https://www.gov.uk/government/publications/dfe-external-data-shares>

Requesting access to your personal data

Under data protection legislation, parents / carers have the right to request access to information about themselves or their child that we hold. To make a request for your personal information, or be given access to your child's educational record, please contact the school office or the Headteacher.

You also have the right to:

- Object to processing of personal data that is likely to cause, or is causing, damage or distress
- Prevent processing for the purpose of direct marketing
- Object to decisions being taken by automated means
- In certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- Claim compensation for damages caused by a breach of the Data Protection regulations

If you should have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at

<https://ico.org.uk/concerns/>