Sherwood Primary School

Data Protection Policy

October 2025

Data Protection Policy

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

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

Sherwood 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) 2018, the UK General Data Protection Regulation (UK GDPR) and with other relevant legislation

Data Protection Principles

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

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)

1. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

2. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

3. Accurate and, where necessary, kept up to date

4. 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

5. 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. Please see Appendix A.
- 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: dataservices@judicium.com
Data Protection Lead for Sherwood Primary School: b.galea@sherwood.lancs.sch.uk

Mrs J Lumb
Headteacher

Mrs E Cockburn-Hyde
Chair of Governors

Date of Policy: October 2025
Date Review Due: October 2027

Appendix A

Subject Access Requests

You have the right to ask Sherwood Primary School if we are using or storing your or your child's personal information. You can also ask for copies of your or your child's personal information.

This is called the right of access and is also known as making a **subject access request**, a **SAR.**

We suggest that you include the following information in your SAR that should be addressed to the Data Protection Officer of Sherwood Primary School:

- a subject line or header that says "subject access request";
- the date you're making the request;
- your name;
- your email address, home address and phone number;
- your child's name;
- what information you want (be specific about the information you're asking for, and where relevant say what information you don't need);
- details or dates that will help us to find the information you want;
- the reason you want the information (you don't have to include this but it will help us to find what you need); and
- if you have any accessibility requirements.

If you exercise any of your rights under data protection law, we respond as quickly as possible. This will be no later than one calendar month, starting from the day we receive the request.

Please note: If we need something from you to be able to deal with your request, the time limit will begin once we have received this.

If your request is complex or you make more than one, the response time may be a maximum of three calendar months, starting from the day of receipt.

What is a calendar month?

A calendar month starts on the day we receive the request, even if that day is a weekend or public holiday. It ends on the corresponding calendar date of the next month.

However, if the end date falls on a Saturday, Sunday or bank holiday, the calendar month ends on the next working day.

Also, if the corresponding calendar date does not exist because the following month has fewer days, it is the last day of the month.

Can I ask for all the information Sherwood Primary School holds about me or my child?

You can ask for all the information we hold about you. However, this doesn't mean you will get all the information we have about you or your child.

We may withhold some, or all, of your or your child's personal information because of an exemption. Exemptions are in the law to protect particular types of information or how certain organisations work.

When we use an exemption, we will:

- tell you why they are not completing your request for information;
- explain their decision; and
- tell you how you can challenge their decision (eg by submitting a complaint).

Sometimes it's acceptable for us to refuse some or all of your request without telling you why.

We don't always need to tell you if we do or don't hold the requested information.

Here are some common exemptions:

'Manifestly unfounded' requests

Manifestly unfounded means that we believes you're not making a SAR because you truly want to exercise your legal right of access.

Examples of when your request may be manifestly unfounded include:

- having no clear intention of exercising your right of access (eg if you make a request but then offer to withdraw it in return for some form of benefit from the Sherwood Primary Schoo); or
- if you are using your request to harass an organisation or cause disruption.

To come to this decision, we will consider each request on a case-by-case basis. We will explain our reasoning to you and the ICO if necessary.

'Excessive' requests

There is no set meaning of what makes a subject access request 'excessive'. However, we will consider whether the request is clearly unreasonable.

Examples of when your request may be excessive include when:

- it overlaps with other, previous requests for similar information (particularly if we haven't had the chance to respond to your first request); or
- your request asks for the same information as previous requests, but not enough time has passed (eg you're aware your information hasn't changed).

To come to this decision, we will consider each request on a case-by-case basis. We will explain our reasoning to you.

Information about other people: Members of staff, children or other people associated with Sherwood Primary School

Responding to a SAR may involve giving out information about other people. We respect your right to get copies of your or your child's information. However, we must also protect other people's rights over their information. This means that if another person's information is included in the requested documents (eg that of another pupil, family member or member of staff), the organisation might redact it or not provide it at all.

However, you may receive information which identifies another person in response to your SAR if:

- that person gives their permission; or
- it is reasonable to comply with your request without the other person's permission.

Legal professional privilege

If your or your child's personal information is discussed or included in confidential communications between the organisation and legal advisors (including in-house legal teams), we don't have to give it to you as part of your request. This information is considered 'privileged', which means it should remain confidential between Sherwood Primary School and the legal team.