



Data Protection Policy

April 2018

Version	Date	Author	Status	Summary
1.0	April 2018	W.Southgate		Linked to Privacy notices Updated in line with new GDPR guidelines May 2018

Reviewed By: Full Governing Body

Date of Review: April 2018

Expiry Date: April 2020

Southwood Infant School Data Protection Policy

At Southwood Infant School (“the school”), we collect and use personal information (referred to in the General Data Protection Regulation (GDPR) as personal data) about staff, pupils, parents, governors, volunteers, third party contractors and suppliers, and other individuals who come into contact with the school. This information is gathered to:

- enable the provision of education to the pupils in the school
- ensure their welling-being and safety
- support their social, moral, cultural, spiritual, and economic development
- make them junior school read
- enable them to participate in and contribute to the wider community
- and for other associated purposes

We also collect information for purposes associated with the provision of the above including administration of employment contracts, staff pay and performance, staff health and well-being, staff development, administration of third party contracts, and the provision of services to the school that support the main education function.

In addition, we are required to by law to collect, use and share certain information, including, for example, pupil performance data, attendance data, and equalities data, with (amongst others) the Department for Education and our local education authority.

The school is the Data Controller, of the personal data that it collects and receives for these purposes.

The school has a Data Protection Officer, who may be contacted at adminoffice@southwood.hants.sch.uk or via the school office on 01252 375420.

The school issues Privacy Notices to all pupils/parents (and other family members who carry out a parental role in relation to the pupil), staff, volunteers, governors, and third-party suppliers and contractors who engage with the school. (the “Data Subject”). A Privacy Notice is displayed on the school website.

These Privacy Notices summarise the personal information held about the categories of Data Subject listed above, the purpose for which it is held and with whom it may be shared. It also provides information about a Data Subject’s rights in respect of their personal data.

Purpose

This policy sets out how the school deals with personal information correctly and securely and in accordance with the GDPR, and other related legislation.

This policy applies to all personal information however it is collected, used, recorded, and stored by the school and whether it is held on paper or electronically.

What is Personal Information/ data?

Personal information or data means any information relating to an identified or identifiable individual. An identifiable individual is one who can be identified, directly or indirectly by reference to details such as a name, an identification number, location data, an online identifier or by their physical, physiological, genetic, mental, economic, cultural, or social identity. Personal data includes, (but is not limited to), an individual's, name, address, date of birth, photograph, bank details and other information that identifies them.

Special Category Data

Special category data (formerly sensitive personal data) is personal information which is considered to be more sensitive and/or to require more protections. This includes information as to race, ethnic origin politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life; or sexual orientation.

The GDPR prohibits the collection, use and sharing of such information, excepted on specified and limited grounds, including to comply with employment and/or social security law, it is in the vital interests of the data subject, processing is of information has been disclosed publicly by the data subject, it is necessary for preventive medical or occupational health needs, or the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment, processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance, or where consent is given.

Data Protection Principles

The GDPR establishes six principles, as well as a number of additional duties, that must be adhered to at all times:

- Personal data shall be processed lawfully, fairly and in a transparent manner
- Personal data shall be collected for specified, explicit and legitimate purposes. It shall not be further processed in a manner that is incompatible with those purposes (subject to exceptions for specific archiving purposes)
- Personal data shall be adequate, relevant, and limited to what is necessary to the purposes for which they are processed and not excessive
- Personal data shall be accurate and, where necessary, kept up to date;
- Personal data shall be kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
- Personal data shall be processed in a manner that ensures appropriate security of the personal.

Duties

Personal data shall not be transferred to a country or territory outside the European Economic Area (EEA), unless that country or territory ensures an adequate level of data protection.

Data Controllers have a General Duty of accountability for personal data.

Commitment

The school is committed to maintaining the principles and duties in the GDPR. Therefore, the school will:

- Inform Data Subjects of the identity and contact details of the Data Controller.
- Inform Data Subjects of the contact details of the Data Protection Officer.
- Inform Data Subjects of the purposes for which their personal information is being collected and the basis for this.
- Not collect, use, or share Special Category Data unless it falls within one of the specified exceptions under GDPR, has consent, or is otherwise legally obliged to do so.
- Inform Data Subjects when their information is shared, and why and with whom unless the GDPR provides a reason not to do this.
- If the school plans to transfer personal data outside the EEA, the school will inform Data Subjects and provide them with details of where they can obtain information of the safeguards for that information.
- Inform Data Subjects of their rights under GDPR.
- Inform Data Subjects that they may withdraw consent (where relevant) and that if consent is withdrawn that the school will cease processing their data (although that will not affect the legality of data processed up until that point).
- Provide details of the length of time a Data Subject's data will be kept.
- Should the school decide to use a Data Subject's personal data for a different reason to that for which it was originally collected the school shall inform that person and where necessary seek consent for such usage.
- Check the accuracy of the information it holds and review it at regular intervals.
- Ensure that only authorised personnel have access to the personal information whatever medium (paper or electronic) it is stored in.
- Ensure that clear and robust safeguards are in place to ensure personal information is kept securely and to protect personal information from loss, theft, and unauthorised disclosure, irrespective of the format in which it is recorded.

- Ensure that personal information is not retained longer than it is needed.
- Ensure that when information is destroyed that it is done so appropriately and securely.
- Share personal information with others only when it is legally appropriate to do so.
- Comply with the duty to respond to requests for access to personal information (known as Subject Access Requests).
- Ensure that personal information is not transferred outside the EEA without the appropriate safeguards.
- Ensure that all staff and governors are aware of and understand these policies and procedures.

Compliance with GDPR Principles

The school complies with the GDPR Principles and GDPR obligations by:

- Issuing Privacy Notices setting out the personal information it collects. Why it is collected, and with whom/why it is shared.
- Having a Retention Policy which sets out the period for which each category of information is retained and, where appropriate, when its retention is reviewed, which it shares with Data Subjects.
- Ensuring its general school policies are compatible with the provisions of the GDPR.
- Notifying Data Subjects of their rights (via the Privacy Notice) in relation to the data it holds.
- Having clear, specific and transparent Consent to use of personal data agreements which express notice to the Data Subject of their right to withdraw consent, and limiting the usage of Consent agreements.
- Collecting and processing Special Category Data only within the permitted exceptions.
- Having clear Guidance to Staff and others (including Governors) setting out the procedures for collecting, retaining, and sharing personal data in accordance with the GDPR.
- Providing training to staff and governors about the GDPR.
- Carrying out Data Protection Impact Assessments where the use of personal information is likely to result in a high risk to the privacy of individuals and/or otherwise obtaining information confirming compliance with GDPR by third

parties with whom the school contracts or with whom it shares information in order to carry out its role as a school.

- Appointing a Data Protection Officer

Breaches of GDPR

In the event of a data breach occurring, the school will notify the Information Commissioner's Office (ICO) within 72 hours of the breach occurring or within 72 hours of the school becoming aware of the breach.

If the breach represents a high data risk, for example, the publication of personal financial information to a non-authorized third party, the school will, in accordance with GDPR immediately notify the Data Subject of the breach.

The school will thereafter review its procedures to ensure that it minimises the risk of a future similar breach.

Complaints

Complaints will be dealt with in accordance with the school's Complaints policy. Complaints relating to the handling of personal information may be referred to the Information Commissioner who can be contacted at Wycliffe House, Water Lane Wilmslow Cheshire SK9 5AF or at www.ico.gov.uk.

Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years. The policy review will be undertaken by the Data Protection Officer, Head teacher, and/or or nominated governor representative.

Contacts

If you have any enquires in relation to this policy, please contact the Data Protection Officer who will also act as the contact point for any queries.

Approved on: April 2018

Review Date: April 2020