



TWESELDOWN INFANT SCHOOL

Data Protection and UK GDPR Policy

1. Introduction

The school collects and uses personal information (referred to UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 as personal data) about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable the provision of education and other associated functions. In addition, the school may be required by law to collect, use and share certain information.

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

The school has an appointed Data Protection Officer (DPO) who is responsible for monitoring compliance with UK GDPR and the Data Protection Act 2018, providing advice to the school and acting as the first point of contact for the Information Commissioner's Office (ICO). This is our Senior Administrative Officer and can be contacted on 01252628843.

The school publishes and regularly reviews Privacy Notices for pupils, parents, staff, governors and volunteers. Privacy Notices will be readily available through the school website and other appropriate channels and will be reviewed at least annually or whenever significant changes are made to processing activities

2. 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 and whether it is held on paper or electronically.

3. What is Personal Information/data?

Personal information or data is 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, and an online identifier or by their physical, physiological, genetic, mental, economic, cultural or social identity. Tweseldown Infant School does not currently hold any biometric data on pupils, staff or Governors. 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.

4. Data Protection Principles

The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018

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 and not 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 purposes identified.**
- **Personal data shall be processed in a manner that ensures appropriate security of the personal data against accidental loss or destruction of, or damage, to personal data.**
- Personal data shall only be transferred outside the UK where appropriate safeguards are in place and where the transfer complies with UK GDPR requirements.
- Data Controllers have a General Duty of accountability for personal data.

5. Commitment

The school is committed to maintaining the principles at all times and duties in the UK GDPR at all times.

Therefore the school will:

- Inform individuals of the identity and contact details of the data controller
- Inform individuals of the contact details of the Data Protection Officer
- Inform individuals of the purposes that personal information is being collected and the basis for this

- Inform individuals when their information is shared, and why and with whom unless the UK GDPR provides a reason not to do this.
- If the school plans to transfer personal data outside the EEA the school will inform individuals and provide them with details of where they can obtain details of the safeguards for the information
- Inform individuals of their data subject rights
- Inform individuals that the individual 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 an individual's data will be kept
- Should the school decide to use an individual's personal data for a different reason to that for which it was originally collected the school shall inform the individual and where necessary seek consent
- Check the accuracy of the information it holds and review it at regular intervals.
- Undertake Data Protection Impact Assessments (DPIAs) where processing activities are likely to result in a high risk to individuals' rights and freedoms, particularly when introducing new technologies, systems, or large-scale processing of personal data.
- 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 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 all staff and Governors are aware of and understand these policies and procedures.
- Ensure all staff complete the annual eLearning for UK GDPR.
- Maintain appropriate technical and organisational measures to safeguard personal data, including password management, multi-factor authentication where appropriate, secure backups, antivirus protection and staff cyber security awareness training.
- • Follow the school's Cyber Security and Online Safety procedures to reduce the risk of unauthorised access, loss or misuse of personal information.

- Personal data will be retained and securely disposed of in accordance with the school's Records Retention Schedule and applicable statutory retention requirements.

Individuals have the following rights under UK GDPR:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure (where applicable)
- Right to restrict processing
- Right to data portability (where applicable)
- Right to object to processing
- Rights relating to automated decision making and profiling

Data Breaches

- The school maintains procedures for identifying, reporting, recording and investigating personal data breaches.
- Any actual or suspected data breach must be reported immediately to the Headteacher and Data Protection Officer.
- Where a breach is likely to result in a risk to the rights and freedoms of individuals, the school will notify the Information Commissioner's Office without undue delay and, where feasible, within 72 hours of becoming aware of the breach.
- Where a breach is likely to result in a high risk to the rights and freedoms of affected individuals, those individuals will be informed without undue delay.
- The school will maintain a record of all personal data breaches, including those that do not require notification to the ICO and report to FGB yearly.

6. 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

7. Contacts

If you have any enquiries in relation to this policy, please contact the Head Teacher who will also act as the contact point for any subject access requests.

8. Review

This policy will be reviewed annually, or sooner where there are changes in legislation, ICO guidance, DfE requirements or school practice.

Date of review: Spring 2024

Date Ratified by Governing Board: Spring 2024

Signed by Chair of Governors:



Signed by Headteacher:

Kim Tottem

Next review date: Spring 2026

Member of staff responsible: Headteacher

Governing Body or Governor(s) /
Committee(s) responsible: Governing Body

Linked documents:

Privacy Notices

MOPP (Manual of Personnel Practice)