

Fleet Wood Lane School

GDPR and Data Protection Policy

2026 – 2027

'Growing our Future Together.'

Approved by:	Full Governing Body	**Date approved:**	_____
Last reviewed on:	_____	**Next review due by:**	Autumn Term 2027
Policy owner:	Data Protection Officer (DPO)	**Version:**	2.0

1. Introduction

Fleet Wood Lane School ("the School") is committed to protecting the personal data of pupils, parents, staff, governors, volunteers and others in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

The School recognises that personal data is essential to delivering education, safeguarding pupils and fulfilling its legal and statutory obligations. The School will process personal data lawfully, fairly and transparently, and will ensure appropriate security and governance measures are in place.

This policy is intended to ensure that personal information is dealt with properly and securely, and in accordance with the legislation. It applies to personal information regardless of how it is used, recorded or stored, and whether it is held in paper files or electronically.

The Information Commissioner's Office (ICO), as the UK's independent supervisory authority, can impose fines of up to £17.5 million, or 4% of an organisation's total annual worldwide turnover in the preceding financial year, whichever is greater, for serious breaches of the UK GDPR. All staff must read, understand and comply with this policy.

2. Scope

This policy applies to:

- All staff (permanent, temporary and supply)
- Governors and trustees
- Volunteers
- Contractors and service providers, including IT and cloud service providers
- Any other person processing personal data on behalf of the School

It applies to personal data held:

- Electronically, including on cloud systems and third-party platforms
- On paper
- In photographs, video, CCTV and other media

The School collects and processes a large amount of personal data, including pupil records, staff records, governor records, safeguarding records, references, payment information, and data required to comply with statutory obligations to the Local Authority, the Department for Education (DfE) and other bodies.

3. Key Definitions

Personal data: Any information relating to an identified or identifiable living individual, including an identifier such as a name, identification number, location data or online identifier.

Special category data: Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health data, genetic data, or biometric data used for the purpose of uniquely identifying an individual, and data concerning a person's sex life or sexual orientation.

Criminal offence data: Personal data relating to criminal convictions and offences, or related security measures (for example, safeguarding case files and DBS check outcomes). This is treated similarly to special category data under Article 10 UK GDPR and Schedule 1 DPA 2018, and requires its own lawful condition for processing.

Processing: Any activity involving personal data, including collecting, recording, storing, using, sharing, restricting or deleting it.

Data subject: The living individual to whom the personal data relates.

Data controller: The organisation that determines the purposes and means of processing personal data. The School is the data controller for the personal data of its pupils, parents, staff and governors.

Data processor: An organisation that processes personal data on behalf of, and under the instruction of, the data controller (for example, a payroll provider or cloud IT platform).

Data Protection Officer (DPO): The person appointed to provide independent advice and monitoring of the School's data protection compliance, and to act as a contact point for the ICO and for data subjects.

A full glossary of further terms is provided at the end of this policy.

4. Data Protection Principles

The School will ensure that personal data is:

- 1. Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency)
- 2. Collected for specified, explicit and legitimate purposes, and not further processed in a manner incompatible with those purposes (purpose limitation)
- 3. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (data minimisation)
- 4. Accurate and, where necessary, kept up to date, with reasonable steps taken to erase or rectify inaccurate data without delay (accuracy)
- 5. Kept in a form which permits identification of data subjects for no longer than is necessary (storage limitation)
- 6. Processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage (integrity and confidentiality)

The School must also be able to demonstrate compliance with each of these principles (accountability), and will maintain documentation to evidence this.

5. Lawful Bases for Processing

Before any new processing activity begins, and periodically thereafter, the purpose and the most appropriate lawful basis (or bases) under Article 6 UK GDPR must be identified and documented. The School relies on the following lawful bases where appropriate:

- Public task – processing necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the School (for example, delivering education)
- Legal obligation – processing necessary to comply with a legal obligation (for example, safeguarding duties, census returns, employment law)
- Contract – processing necessary for the performance of a contract, or to take steps at the request of the data subject prior to entering into a contract (for example, employment contracts)
- Vital interests – processing necessary to protect the vital interests of the data subject or another individual
- Legitimate interests – processing necessary for the legitimate interests of the School or a third party, save that this basis does not apply to processing carried out by the School in the exercise of its public task functions, and may only be relied on for other, non-public-task activities following a documented legitimate interests assessment

- Consent – the data subject has given clear, informed and freely given consent to processing for one or more specific purposes. Consent must be capable of being withdrawn at any time, and withdrawal must be honoured promptly

The lawful basis relied upon, and the purpose of the processing, must be recorded and set out in the School's relevant privacy notice(s). Where processing is likely to result in a significant privacy impact, a Data Protection Impact Assessment (DPIA) must also be carried out (see Section 7).

6. Special Category and Criminal Offence Data

Processing of special category data is prohibited unless a lawful basis under Section 5 applies and one of the following specific conditions under Article 9 UK GDPR is also met:

- (a) the individual has given explicit consent, clearly explained in a privacy notice
- (b) the processing is necessary for employment law purposes
- (c) the processing is necessary to protect the vital interests of a data subject who is physically or legally incapable of giving consent
- (d) the processing is carried out by a not-for-profit body with a political, philosophical, religious or trade-union aim, in the course of its legitimate activities and with appropriate safeguards
- (e) the processing relates to personal data manifestly made public by the data subject
- (f) the processing is necessary for the establishment, exercise or defence of legal claims
- (g) the processing is necessary for reasons of substantial public interest
- (h) the processing is necessary for preventative or occupational medicine, or the assessment of working capacity
- (i) the processing is necessary for reasons of public interest in the area of public health

Criminal offence data (including safeguarding case files and DBS outcomes) may only be processed where a condition under Schedule 1 DPA 2018 applies, in addition to an Article 6 lawful basis. Evidence of the condition relied upon must be recorded.

Biometric data

Where the School processes biometric data of pupils under 18 (for example, fingerprint recognition for cashless catering or library systems), it must also comply with Section 26 of the Protection of Freedoms Act 2012. This requires written parental consent before a pupil's biometric data is taken, gives either parent the right to object even where the other parent has consented, and requires the School to provide a reasonable alternative means of accessing the service for any pupil whose biometric data is not processed.

7. Data Protection Impact Assessments (DPIA)

The School will implement 'privacy by design' when processing personal data, embedding privacy considerations and appropriate technical and organisational measures (such as pseudonymisation) into its processes from the outset.

Where processing is likely to result in a high risk to individuals' data protection rights (for example, the introduction of new technology or a new data-sharing arrangement), a DPIA must be carried out to assess:

- Whether the processing is necessary and proportionate to its purpose
- The risks to individuals
- What measures can be put in place to address those risks

Staff should refer to the DfE's Data Protection Toolkit for Schools and consult the DPO when carrying out a DPIA. Completed DPIAs must be signed off by the DPO.

8. Documentation and Records of Processing

The School will maintain written records of its processing activities, including:

- The purposes of the processing and the categories of personal data and individuals involved
- The lawful basis (and, where applicable, special category condition) relied upon
- Categories of recipients, including any processors and third countries
- Retention periods
- A description of technical and organisational security measures
- Records of consent, DPIAs, controller-processor contracts, and data breaches

These records will be reviewed regularly, including through information audits, discussions with staff about their processing activities, and review of relevant policies and contracts.

9. Privacy Notices

The School will issue privacy notices to inform data subjects (or, for pupil data, their parents, subject to the pupil's age and understanding) about what personal data is collected, how it is used, the lawful basis relied upon, and their rights.

Where data is collected directly from the individual, the privacy notice must be provided at the point of collection. Where data is collected indirectly (for example, from a third party), the notice must be provided as soon as reasonably possible thereafter. Privacy notices will be written in clear, plain language.

10. Purpose Limitation and Data Minimisation

Personal data must be collected only for specified, explicit and legitimate purposes, and must not be used for a new or incompatible purpose unless the data subject has been informed and, where necessary, has consented.

Personal data must be adequate, relevant and limited to what is necessary. Staff may only access and process personal data that their role requires, and must not use personal data for any purpose unrelated to their role. Data no longer required will be deleted in line with the School's Records Retention Schedule.

11. International Data Transfers

The School generally processes personal data within the UK. Where personal data is transferred outside the UK (including where a cloud or software provider stores or accesses data on servers located overseas), the transfer must comply with Chapter V UK GDPR. A transfer may only take place where:

- The destination country is covered by UK adequacy regulations made by the Secretary of State, or
- Appropriate safeguards are in place, such as the ICO's International Data Transfer Agreement (IDTA), the UK Addendum to the EU Standard Contractual Clauses, or Binding Corporate Rules, or
- A specific derogation applies, such as the explicit informed consent of the data subject

This is particularly relevant to cloud-based and EdTech platforms used by the School (for example, Microsoft 365, Google Workspace for Education, and other online learning or communication tools), many of which involve some processing outside the UK. Staff must not sign up to, or begin using, any new online platform or service that processes personal

data without first checking with the DPO that an appropriate transfer mechanism and data processing agreement are in place.

12. Roles and Responsibilities

Governing Body

- Provides strategic oversight of data protection compliance and ensures the School has adequate resources and policies in place.

Headteacher

- Has day-to-day responsibility for ensuring the School complies with this policy and with data protection law.

Data Protection Officer (DPO)

- Provides independent advice on data protection matters, including DPIAs
- Monitors compliance with this policy and with data protection law
- Acts as the first point of contact for the ICO and for data subjects exercising their rights
- Signs off DPIAs and advises on new processing activities, contracts and data-sharing arrangements

DPO contact details: [Insert name / job title / organisation / email / phone]

All Staff, Governors, Volunteers and Contractors

- Must read, understand and comply with this policy
- Must only access personal data they are authorised to access, and only for authorised purposes
- Must report any actual or suspected data breach immediately, in accordance with Section 18
- Must not remove personal data, or devices containing personal data, from School premises unless appropriate security measures (such as encryption or password protection) are in place
- Must not store personal data on local drives, personal devices, or personal cloud accounts

13. Data Subject Rights

Individuals have the following rights in relation to their personal data under UK GDPR:

- To be informed about how, why and on what basis their data is processed
- To access their personal data by making a Subject Access Request (see Appendix 1)
- To have inaccurate or incomplete data corrected (rectification)
- To have data erased where it is no longer necessary, or there are no overriding grounds for processing ('right to be forgotten')
- To restrict processing in certain circumstances, including where accuracy is contested or processing is unlawful
- To receive or request the transfer of their data to a third party in a structured, machine-readable format, where applicable (data portability)
- To withdraw consent to processing at any time, where consent is the lawful basis relied upon
- To object to decisions based solely on automated processing, including profiling
- To be notified of a data breach likely to result in a high risk to their rights and freedoms
- To complain to the ICO or to a court

The School will respond to requests within the statutory timeframes set out in Appendix 1, and in accordance with its procedures.

14. Data Security

Staff must maintain the confidentiality, integrity and availability of personal data:

Confidentiality: only people who have a need to know, and are authorised, can access the data

Integrity: the data is accurate and suitable for the purpose for which it is processed

Availability: authorised users can access the data when they need it for authorised purposes

The School implements appropriate technical and organisational measures, including:

- Role-based access controls and least-privilege access
- Secure passwords, multi-factor authentication and account management
- Encryption and pseudonymisation where appropriate
- Secure configuration of cloud systems and regular review of third-party app permissions
- Physical security of paper records and School premises
- Secure disposal of records (for example, shredding or certified destruction)
- Regular staff awareness training

Where an external organisation processes personal data on the School's behalf, a written contract must be in place requiring the processor to act only on the School's instructions, maintain confidentiality, implement appropriate security, only engage sub-processors with the School's prior consent, assist with subject access and other data subject rights, delete or return data at the end of the contract, and notify the School immediately of any breach. New processor agreements must be approved by the DPO before being entered into.

15. Data Sharing

Where the School shares personal data with third parties (including the Local Authority, other schools, health and social care agencies, or the police), such sharing will be lawful, necessary and proportionate, and due diligence will be carried out on the recipient.

Data protection law does not prevent the School from sharing information for safeguarding purposes. Where sharing is necessary to protect a child from harm, the School may rely on the safeguarding-related exemptions in Schedule 2 DPA 2018 and need not always seek consent, provided the sharing is necessary and proportionate; staff should discuss any safeguarding disclosure with the Designated Safeguarding Lead and, where appropriate, the DPO.

16. Data Retention and Disposal

The School retains personal data only for as long as necessary to fulfil the purpose for which it was collected, or to meet a legal or statutory requirement, in accordance with its Records Retention Schedule (based on the IRMS Records Management Toolkit for Schools). Personal data no longer required will be securely deleted or destroyed, including by third parties holding data on the School's behalf.

17. Data Breach Management

A data breach may include loss or theft of data or equipment, unauthorised access or disclosure, system or hardware failure, human error, or a deliberate attack such as phishing or hacking.

Any actual or suspected data breach must be reported immediately to the Headteacher and/or DPO. On being notified, the School will:

- Investigate the breach and take reasonable steps to contain and recover the data
- Assess the risk to affected individuals' rights and freedoms
- Notify the ICO without undue delay, and where possible within 72 hours, if the breach is likely to result in a risk to individuals
- Notify affected individuals without undue delay if the breach is likely to result in a high risk to their rights and freedoms
- Record every breach – including those not reported to the ICO – in the School's breach log, together with its effects and the remedial action taken

18. Training and Awareness

All staff will receive data protection training as part of induction, with periodic refresher training thereafter. The School promotes ongoing awareness of data protection responsibilities and good practice, and staff with specific data protection responsibilities (such as SENCOs, the DSL, and office staff handling SARs) will receive role-appropriate additional training.

19. Consequences of Non-Compliance

The School takes compliance with this policy very seriously. Failure to comply puts data subjects at risk and may expose the individual and the School to civil and criminal sanctions. Any failure to comply may lead to disciplinary action under the School's procedures, which may result in dismissal for gross misconduct. Where a non-employee breaches this policy, their contract may be terminated with immediate effect.

20. Monitoring and Review

The DPO will monitor compliance with this policy through internal review and will report significant issues to the Governing Body. This policy will be reviewed annually, or sooner if there is a significant change to data protection law, guidance, or the School's processing activities.

21. The Supervisory Authority in the UK

The Information Commissioner's Office (ICO) is the UK's independent supervisory authority for data protection. The ICO's website (https://ico.org.uk/) provides detailed guidance on individuals' rights, data breach reporting, handling Subject Access Requests, and other data protection topics.

22. Glossary

Automated Decision-Making (ADM): A decision based solely on automated processing (including profiling) that produces legal effects or significantly affects an individual. UK GDPR restricts ADM unless certain conditions are met.

Consent: Freely given, specific, informed and unambiguous agreement to processing, given by a clear statement or positive action.

Data Controller: The organisation that determines the purposes and means of processing personal data.

Data Processor: An organisation that processes personal data on behalf of the data controller.

Data Subject: A living, identifiable individual about whom personal data is held.

DPIA: A Data Protection Impact Assessment: a tool used to identify and reduce data protection risks.

EEA: The European Economic Area (EU member states plus Iceland, Liechtenstein and Norway). Note: transfers from the UK are governed by the UK GDPR transfer regime, not EEA rules, following the UK's withdrawal from the EU.

Explicit Consent: Consent expressed by a very clear and specific statement, rather than by another form of positive action.

Personal Data: Information relating to an identified or identifiable living individual, including factual information and expressions of opinion.

Personal Data Breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Privacy by Design: Embedding appropriate technical and organisational measures into processing activities from the outset to ensure compliance with data protection law.

Privacy Notice: A notice provided to data subjects setting out how and why their personal data is used.

Processing: Any operation performed on personal data, including collection, storage, use, disclosure, restriction or erasure.

Pseudonymisation: Replacing identifying information with an artificial identifier, so that additional information (kept separately and securely) is needed to re-identify the individual.

Special Category Data: Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health data, genetic or biometric data used for identification, or data concerning sex life or sexual orientation.

UK GDPR: The retained EU General Data Protection Regulation (EU 2016/679) as it forms part of UK domestic law, as amended, read together with the Data Protection Act 2018.

Appendix 1: Subject Access Request (SAR) Procedure

Any individual - or a parent/carer with parental responsibility acting on a pupil's behalf may request access to personal data held by the School by making a Subject Access Request (SAR).

1. How Requests May Be Made Requests can be submitted verbally or in writing (by letter, email, or social media) to any member of staff, and do not need to use specific legal terminology or name the Data Protection Officer (DPO).

2. Immediate Staff Actions on Receipt On receiving a SAR, staff must immediately pass the request to the **Headteacher**, noting the exact date of receipt. Staff must not attempt to respond to, fulfil, or refuse a request themselves.

3. Operational Management & Logging

Upon receipt, the **Headteacher** (or designated office administrator) will:

- Record the request in the school's central **SAR Register** to calculate and track statutory response deadlines.
- Notify the external **DPO** for advice, guidance, and sign-off on disclosures, complex requests, or potential exemptions.

4. School Fulfilment Procedure

The School will:

- **Verify Identity:** Confirm the identity of the requester and verify parental responsibility before releasing personal data.
- **Timeframe:** Respond within **one calendar month** of receiving a valid request and identity verification.
- **Extensions:** Extend the response period by up to **two additional months** for complex or numerous requests, informing the requester of the delay and reasons within the first month.
- **Fees:** Provide the information **free of charge**, unless the request is manifestly unfounded or excessive, in which case a reasonable administrative fee may be charged or the request refused (with written reasons provided).
- **Redactions & Exemptions:** Withhold or redact information that is exempt from disclosure under the Data Protection Act 2018 (such as third-party personal data or information subject to safeguarding/legal exemptions) in consultation with the DPO.

5. Statutory Educational Records Requests

Requests made by parents purely to inspect or receive paper copies of a pupil's official educational record under the *Education (Pupil Information) (England) Regulations 2005* are handled separately. These must be submitted in writing to the Headteacher and processed within **15 school days**.

6. Complaints & Appeals If a requester is dissatisfied with how their SAR was handled, they may request an internal review by contacting the Governing Body. Requesters also maintain the statutory right to lodge a complaint directly with the **Information Commissioner's Office (ICO)** via ico.org.uk/concerns or by calling 0303 123 1113.