New Woodlands School Data Protection Policy (UK GDPR)

Version 5.0 | Effective: 2025-08-19 | Review: Annually or on change

Document control

Owner: Data Protection Officer (DPO)
Approver: Headteacher & Governing Board
Supersedes: IDP-0518-A004_Data Protection Policy GDPR V4 (2018)

1. Purpose and scope

This Policy sets out how [School Name] complies with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018) when handling personal data relating to pupils, parents/carers, employees, governors, contractors, volunteers and other individuals. It applies to all personal data processed by or on behalf of the school, in any format (paper, electronic, images, audio/visual) and in any location (on-premise, cloud, portable devices).

2. Definitions (plain English)

Personal data: any information about an identifiable living person.

Special category data: health, ethnicity, religion, biometrics for ID, genetics, sex life/sexual orientation, political opinions, trade union membership.

Criminal offence data: convictions/allegations; processed only with a Schedule 1 DPA 2018 condition and Appropriate Policy Document.

Processing: anything done with personal data.

Controller/Processor: the school is usually the Controller; third parties may act as Processors under contract.

3. Our data protection principles

We commit to the six principles: lawfulness, fairness & transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity & confidentiality (security); and the accountability obligation that underpins them.

4. Lawful bases

We identify and document a lawful basis for each processing activity (e.g., public task, legal obligation, vital interests, contract, consent, legitimate interests where applicable). Special category data also needs an Article 9 condition; criminal offence data a Schedule 1 DPA 2018 condition and an Appropriate Policy Document.

5. Roles and responsibilities

Governing Board: oversight and resources.

Headteacher: operational compliance and culture.

Senior Information Risk Owner (SIRO): information risk management.

Data Protection Officer (DPO): independent advisor, contact for ICO and data subjects; consulted on DPIAs.

Information Asset Owners (IAOs): responsible for systems (MIS, HR, Safeguarding).

All staff & volunteers: complete training; follow policy; report incidents immediately.

6. Transparency and privacy notices

We provide clear, age-appropriate privacy notices explaining identity, purposes, lawful bases, recipients, retention, rights, DPO contact and any international transfers. Children's notices use plain, age-appropriate language. If relying on consent for information society services, UK age of consent is 13.

7. Individual rights

We enable rights to access, rectification, erasure, restriction, portability (where applicable), objection, and rights in relation to automated decisions/profiling. We respond within one month (extendable by two months for complex/multiple requests). No fee unless manifestly unfounded or excessive. Parents in maintained/special schools may access the pupil's education record within 15 school days; copying charges may apply.

8. Data sharing and disclosures

We share data when lawful and necessary (e.g., safeguarding, statutory returns, educational provision), ensuring proportionality and minimum necessary disclosure. Processor relationships are governed by Article 28 contracts; new routine sharing may be supported by a Data Sharing Agreement.

9. International transfers

We use appropriate safeguards—UK adequacy, the UK International Data Transfer Agreement (IDTA) or UK Addendum to the EU SCCs—and complete a Transfer Risk Assessment before transfers outside the UK.

10. Security (technical and organisational measures)

We maintain layered controls: access control/least privilege, MFA, encryption at rest/in transit, secure configuration and patching, logging/monitoring, secure disposal, physical security, tested backup/restore, secure email and redaction, MDM on devices, removable media controls, and supplier due diligence. Staff must use only authorised systems and keep accounts/devices secure.

11. Records of Processing Activities (ROPA)

We maintain a current ROPA describing purposes, categories, recipients, transfers, retention, security measures and lawful bases; reviewed at least annually and whenever processing changes.

12. Data Protection Impact Assessments (DPIAs)

We complete a DPIA for high-risk processing (e.g., innovative technologies/AI, biometrics, large-scale special category data, systematic monitoring/CCTV). If residual risk remains high, we consult the ICO before proceeding.

13. Retention and disposal

We retain data only as long as necessary and follow our Records Management & Retention Schedule; we securely delete or anonymise data when no longer needed and log routine destruction.

14. Data breaches and incident response

All suspected personal data breaches must be reported immediately. If a breach is likely to risk individuals' rights and freedoms, we notify the ICO without undue delay and within 72 hours of awareness; if high risk, we also inform affected individuals without undue delay. We keep a central breach log and implement lessons learned.

15. Training and awareness

All staff and governors complete induction and annual refresher training; role-based training for IAOs, admins and safeguarding teams. Completion is monitored and reported.

16. Monitoring, audit and review

We monitor compliance via spot checks, access audits, supplier reviews, and periodic audits. This policy is reviewed annually or on significant change.

17. Related policies and procedures

Information Security Policy; Records Management & Retention; CCTV/Monitoring; Appropriate Policy Document; Data Breach Response Procedure; SAR Procedure; FOI Publication Scheme & Procedure; Acceptable Use & Remote Working.

18. Contact

DPO: Stephen Williams

T: 0208 314 6212

E: dpo@lewisham.gov.uk