

Larkfield Primary School

Data Protection Policy



Approved by:	Dave Palmen	Date:	21st October 2026
Last reviewed on:	21st October 2026	Next review due by:	31st October 2027

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection legislation. This includes the UK General Data Protection Regulation (UK-GDPR), the Data Protection Act 2018 (DPA 2018), and the Data (Use and Access) Act 2025. This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and Guidance

This policy meets the requirements of current UK data protection legislation, including:

- **UK-GDPR** and the **Data Protection Act 2018**
- **Data (Use and Access) Act 2025**
- Guidance published by the Information Commissioner's Office (ICO) and the Department for Education (DfE)
- The ICO's codes of practice, including surveillance camera usage and the Children's Code
- Regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record

3. Definitions

Term	Definition
Personal data	Any information relating to an identified or identifiable living individual. This includes names, identification numbers, location data, online identifiers, or factors specific to physical, physiological, genetic, mental, economic, cultural, or social identity.
Special categories of personal data	Personal data that is particularly sensitive and requires higher protection, including racial/ethnic origin, political opinions, religious/philosophical beliefs, trade union membership, genetic/biometric data (where used for identification), physical/mental health data, or

Term	Definition
	sex life/sexual orientation.
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disclosing, erasing, or destroying. Can be automated or manual.
Data subject	The identified or identifiable living individual whose personal data is held or processed.
Data controller	An organisation or entity that determines the purposes and means of processing personal data.
Data processor	A person or entity (other than an employee) who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
Artificial Intelligence (AI) System	Software or algorithmic tools that process input data to generate outputs such as content, predictions, recommendations, or automated decisions.

4. The Data Controller

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school is registered with the Information Commissioner's Office (ICO) and pays its data

protection fee annually as required by law.

5. Roles and Responsibilities

This policy applies to all staff employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Governing Board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2 Data Protection Officer (DPO)

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law, and developing related policies and guidelines where applicable. They provide an annual report of activities directly to the governing board and advise on school data protection matters.

The DPO is the primary contact for individuals whose data the school processes and for the ICO.

Our DPO is **Mr Nick Holden (NexusProtect)**, contactable on **08454 631072** or **governance@nexus-global.co.uk**.

5.3 Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis.

5.4 All Staff

Staff are responsible for:

- Collecting, storing, and processing personal data in accordance with this policy
- Informing the school of any changes to their personal data (e.g. change of address)
- Contacting the DPO in the following circumstances:
 - With any questions about data protection law, retention, or security
 - If they suspect or confirm a data protection breach has occurred
 - If unsure about a lawful basis or when engaging new tools (including AI platforms)
 - Before transferring personal data outside the UK
 - When entering into new contracts or data-sharing agreements with third parties

6. Data Protection Principles

The school complies with the fundamental data protection principles, ensuring personal data is:

- Processed lawfully, fairly, and in a transparent manner
- Collected for specified, explicit, and legitimate purposes
- Adequate, relevant, and limited to what is necessary
- Accurate and, where necessary, kept up to date
- Kept for no longer than necessary for the processing purposes
- Processed securely using appropriate technical and organisational measures

7. Collecting Personal Data

7.1 Lawfulness, Fairness, Transparency, and Recognised Legitimate Interests

We only process personal data where we have a lawful basis under UK data protection law (contract, legal obligation, vital interests, public task, legitimate interests, or consent). In accordance with the Data (Use and Access) Act 2025, processing undertaken for emergency response, safeguarding pupil safety, or crime prevention is classified under recognized legitimate interests, streamlining procedures where urgent protective action is required. When collecting data directly, we provide clear privacy notices. We ensure data processing is fair, transparent, and within reasonable expectations.

7.2 Limitation, Minimisation, and Accuracy

Personal data is collected only for specified purposes and kept accurate and up to date. Inaccurate data is rectified or erased promptly. Data no longer required is deleted or anonymised in accordance with the school retention schedule.

8. Sharing Personal Data

We do not share personal data without consent unless legally required or permitted. Circumstances include:

- Safeguarding or risk to safety of staff/pupils
- Liaison with statutory bodies, local authorities, or emergency services
- Contractors and IT suppliers providing services (under binding data processing agreements)
- Law enforcement bodies as required by law

International transfers of data outside the UK are strictly conducted in accordance with the UK Data Bridge framework and UK Data Protection Test.

9. Subject Access Requests (SARs) and Individual Rights

9.1 Subject Access Requests (SARs)

Individuals have a right to request access to their personal data held by the school. In line with the Data (Use and Access) Act 2025:

- **Proportionate Searches:** The school is required to conduct reasonable and proportionate searches for requested records.
- **Clarification & "Stop-the-Clock":** Where a request is broad or ambiguous, the school may request clarification from the applicant. The statutory 1-month timeframe for responding is paused ("stop-the-clock") from the date clarification is requested until it is received.

9.2 Children and Subject Access Requests

Personal data belongs to the child. Parents/carers may exercise SAR rights on behalf of children under 12 who lack the maturity to understand their rights, evaluated on a case-by-case basis.

9.3 Responding to SARs

We respond without delay and within 1 month of receipt (excluding paused clarification windows). Requests are free of charge unless unfounded, repetitive, or excessive, in which case reasonable administrative fees or refusals apply with full written justification provided.

9.4 Other Individual Rights

Data subjects also hold rights to rectification, erasure ("right to be forgotten"), restriction, objection, data portability, and human review for automated decisions.

10. Data Protection Complaints Procedure

The school maintains a dedicated procedure for handling data protection concerns:

1. Complaints regarding data processing should be submitted in writing to the DPO at governance@nexus-global.co.uk.
2. The school will formally acknowledge receipt of the complaint within **30 days** and outline the investigation timeline.
3. If unsatisfied with the outcome, individuals may escalate their complaint directly to the Information Commissioner's Office (ICO) at ico.org.uk.

11. Parental Requests to See Educational Records

Parents or carers with parental responsibility have a statutory right to free access to their child's educational record within 15 school days of a written request, subject to legal withholding exemptions (e.g. serious risk of harm).

12. Artificial Intelligence (AI) and Automated Decision-Making

When implementing educational technology, software, or AI tools:

- **DPIA Requirement:** A Data Protection Impact Assessment (DPIA) must be completed prior to adopting any AI system that processes personal data.
- **Prohibition of Solely Automated Decisions:** No decision producing legal or significant effects on pupils or staff will be made solely by automated algorithms or AI systems without human intervention.
- **Data Privacy:** Pupil data must not be used to train external public AI models.

13. Data Protection by Design and Default

Data protection measures are integrated into all processing activities. DPIAs are mandatory for high-risk operations or new technology integrations. Annual data protection training is mandatory for all staff and governors.

14. Technical Security and Data Storage

We maintain robust technical security measures to protect personal data:

- **Password & Passphrase Policy:** Device and account passwords must follow NCSC guidance using strong passphrases (e.g. 3 random words). Simple character rules that encourage weak patterns are prohibited.
- **Multi-Factor Authentication (MFA):** MFA is mandatory across all staff accounts accessing cloud services, emails, or school systems off-site.
- **Encryption:** Full-disk encryption is mandatory for all portable laptops, mobile devices, and removable storage media.
- **Clear Desk Policy:** Confidential physical files must be locked in cabinets when unattended.

15. Disposal of Records

Records are securely disposed of (shredding/degaussing/overwriting) in accordance with the school's retention schedule once no longer required.

16. Personal Data Breaches

In the event of a personal data breach, staff must immediately inform the DPO. The DPO will assess risks, contain the incident, and report to the ICO within ****72 hours**** where required. High-risk breaches will be communicated promptly to affected individuals.

17. Training and Monitoring

All staff receive data protection training upon induction and annually thereafter. This policy is reviewed ****annually**** by the DPO and Headteacher and submitted to the Governing Board for approval.

18. Links with Other Policies

- Child Protection & Safeguarding Policy
- Online Safety Policy
- Freedom of Information Publication Scheme
- AI & Educational Technology Usage Policy