Little Kingshill Combined School
Data Protection Policy

Version Control

Version	Date	Change summary
v3.0	February 2026	Comprehensive update for DUAA 2025 (in force 5 Feb 2026): SARs "stop the clock", recognised legitimate interests, ADM safeguards, purpose compatibility; new Data Protection Complaints section effective 19 June 2026.
v2.0	November 2024	Review and minor updates.
v1.0	September 2018	Policy issued for UK GDPR and DPA 2018.

Table of Contents

Appendix 3: Lawful bases (summary)

1. Aims

Little Kingshill Combined School (LKCS) aims to ensure that all personal data about staff, pupils, parents/carers, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law (UK GDPR and the Data Protection Act 2018), as amended by the Data (Use and Access) Act 2025 (DUAA).

This policy applies to all personal data, regardless of the format (paper or electronic) and regardless of where that data is held.

2. Legislation and guidance

This policy meets the requirements of:

• UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (DPA 2018).

• The Data (Use and Access) Act 2025, including changes commenced on 5 February 2026 affecting, among other things, subject access requests (reasonable and proportionate searches and the ability to “stop the clock”), recognised legitimate interests, automated decision-making (ADM) safeguards, and purpose compatibility. [See GOV.UK DUAA guidance; legal briefings]

• ICO guidance including the Children’s Code (Age Appropriate Design) and updates to subject access guidance. [See ICO Children’s Code strategy updates]

3. Definitions

Definitions (personal data, special category data, processing, data subject, data controller, data processor, personal data breach) follow Article 4 UK GDPR and associated DPA 2018 definitions. See also Section 6 for principles.

4. The data controller

LKCS is the data controller and is registered with the ICO. The school will renew its registration annually or as legally required.

5. Roles and responsibilities

This policy applies to all employees and to external organisations/individuals working on our behalf. Non-compliance may result in disciplinary action or termination of contracts.

• Governing board: Overall responsibility for ensuring compliance with data protection obligations.

• Data Protection Officer (DPO):

Data Protection Officer	Nicola Cook schoolsDPO.com	nicola@schoolsdpo.com	01296 658502

. Oversees implementation, monitors compliance, reports to governors and acts as first point of contact for data subjects and the ICO.

• Headteacher: Acts as the controller's representative on a day-to-day basis (contact via office@lkcs.org.uk).

• All staff: Must collect, store and process personal data in accordance with this policy and contact the DPO where necessary (e.g., questions on lawful bases, contracts, data sharing, international transfers, DPIAs, or in the event of a suspected breach).

6. Data protection principles

LKCS adheres to the UK GDPR principles: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability. Measures to comply are set out throughout this policy.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have a lawful basis under UK GDPR Article 6. In addition to contract, legal obligation, vital interests, public task, legitimate interests and consent, LKCS recognises the DUAA-introduced lawful basis of recognised legitimate interests for defined purposes (e.g., safeguarding vulnerable people, crime prevention, emergencies, certain public interest tasks). Where this narrow basis applies, no balancing test is required, although transparency and necessity still apply. [Recognised legitimate interests under DUAA]

For special category data, we will meet a condition under Article 9 and Schedule 1 DPA 2018. For criminal offence data, we will meet both a lawful basis and a relevant Schedule 1 condition.

Whenever we collect personal data directly, we will provide appropriate privacy information (privacy notices).

7.2 Limitation, minimisation and accuracy

We collect personal data for specified, explicit and legitimate purposes and will not process in ways incompatible with those purposes. We ensure data is adequate, relevant and limited to what is necessary, kept accurate and up to date, and deleted or anonymised when no longer required in line with our retention schedule. We will document our justification for each category of data and conduct regular data minimisation reviews.

8. Sharing personal data

We do not routinely share personal data, but we may do so with third parties where lawful and necessary, including safeguarding partners, law enforcement, local authorities, our processors (e.g., IT service providers), emergency services, and for legal or regulatory obligations. We will have appropriate contracts/data sharing agreements in place and only share what is necessary. Where personal data is transferred outside the UK, we will comply with UK transfer rules.

9. Subject access requests (SARs) and other rights

9.1 Making a SAR

Individuals may request access to their personal data. Requests should be submitted in writing to the DPO and include sufficient details and, where needed, identification/authority.

9.2 Children and SARs

Personal data about a child belongs to that child. We will assess a child's capacity to understand their rights case-by-case (children under 12 are generally unlikely to fully understand their rights).

9.3 Responding to SARs

We will respond without undue delay and within one month of receiving all necessary information. Under the DUAA, we may "stop the clock" while awaiting clarification or ID, and our searches will be "reasonable and proportionate". We may request ID/clarification and will tell the requester if we extend up to a further

two months for complex requests. Information is provided free of charge unless requests are manifestly unfounded or excessive. [DUAA SARs: reasonable/proportionate and stop-the-clock]

We will refuse or limit disclosure where an exemption applies (e.g., serious harm, safeguarding, legal restrictions) and will explain the reasons and the right to complain to the ICO.

9.4 Other rights

Individuals have rights to rectification, erasure, restriction, objection (including to public task/legitimate interests), data portability (where applicable), to prevent direct marketing, to challenge automated decisions/profiling, and to be notified of certain breaches. Requests should be sent to the DPO.

10. Parental requests to see the educational record

Parents/those with parental responsibility have a legal right to free access to the educational record within 15 school days of a written request (Education (Pupil Information) Regulations 2005).

11. CCTV

LKCS uses CCTV in selected areas for site safety and security and follows ICO surveillance guidance. Signs are displayed to inform individuals. Enquiries about CCTV should be directed to the Headteacher via office@lkcs.org.uk.

12. Photographs and videos

We obtain consent from parents/carers for the use of images/video for communication, marketing and promotional purposes. Consent may be withdrawn at any time. Images will not be accompanied by additional personal information to avoid identification. See our safeguarding/photography policies for further details.

13. Data protection by design and default

We integrate data protection into processing activities and projects, including appointing a suitably qualified DPO, ensuring only necessary personal data is processed, conducting DPIAs where processing presents high risks or introduces new technologies, reviewing privacy notices, training staff, and auditing controls.

Where online services are likely to be accessed by children, we will take into account children’s developmental needs and the ICO Children’s Code (Age

Appropriate Design) in our product/service selection, configuration and governance. [Children's Code/DUAA alignment]

14. Data security and storage of records

We protect personal data against unauthorised or unlawful access, alteration or disclosure, and against accidental loss, destruction or damage through technical and organisational measures including:

• Physical security for paper records and devices;

• Clear-desk practices;

• Access controls and least-privilege principles;

• Strong passwords and (where available) multi-factor authentication;

• Encryption for portable devices and removable media;

• Secure configuration, patching and malware protection;

• Due diligence for processors and secure data sharing;

• Staff guidance on using personal devices in line with Acceptable Use/Online Safety policies.

15. Disposal of records

Personal data that is no longer required will be disposed of securely (e.g., shredding, secure disposal, secure deletion/overwriting). Third-party disposal services will provide appropriate assurances of compliance.

16. Personal data breaches

We will take all reasonable steps to prevent personal data breaches and will follow our breach procedure (Appendix 1). Where required, the ICO will be notified within 72 hours and affected individuals informed where there is a high risk to their rights and freedoms.

17. Data protection complaints (effective 19 June 2026)

From 19 June 2026, individuals have a statutory right to complain to the controller about how their personal data has been handled. LKCS will facilitate such complaints and respond without undue delay. Complaints should be submitted to the DPO in the first instance; unresolved complaints may be escalated to the ICO. [DUAA complaints commencement]

How to complain:

• Email the DPO:

Data Protection Officer	Nicola Cook schoolsDPO.com	nicola@schoolsdpo.com	01296 658502

• Write to: Data Protection Officer, Little Kingshill Combined School, [School address]

• If you remain dissatisfied, you may contact the Information Commissioner's Office (www.ico.org.uk).

18. Training

All staff and governors receive data protection training at induction and regular refreshers following legal or policy changes. Attendance is recorded.

19. Monitoring and review

The DPO monitors and reviews this policy. It will be reviewed annually, or sooner if required by changes in legislation or ICO guidance, and shared with the governing board.

20. Links with other policies

This policy should be read with: Freedom of Information Publication Scheme; Acceptable Use of ICT; Child Protection & Safeguarding; Online Safety; CCTV/Surveillance; Records Management and Retention Schedule; Complaints Policy.

Appendices

Appendix 1: Personal data breach procedure

This procedure follows ICO guidance. On discovering or suspecting a breach, staff/processor must immediately notify the DPO. The DPO will assess, contain, investigate, record and, where required, notify the ICO within 72 hours and affected individuals where risk is high. The DPO and Headteacher will review causes and implement improvements (process, training, technical controls).

Examples of school-context breaches include: publication of non-anonymised pupil results; disclosure of safeguarding information to an unauthorised person; theft or loss of an unencrypted device containing personal data. Where mis-sent email contains special category data, recall will be attempted, recipients contacted to delete securely, confirmation obtained, and online publication checks made.

Appendix 2: Automated decision-making (ADM) and profiling

LKCS does not currently make decisions producing legal or similarly significant effects based solely on automated processing. Should this change, LKCS will implement safeguards required by law, including meaningful human intervention, the ability to express a view and contest a decision, and transparency about the logic and consequences. Special category data will not be used for solely automated decisions unless a legal exemption applies. [DUAA ADM safeguards]

Appendix 3: Lawful bases (summary)

Contract; Legal obligation; Vital interests; Public task; Legitimate interests; Consent; Recognised legitimate interests (narrow, DUAA-defined purposes such as safeguarding, crime prevention, emergencies, certain public tasks). Controllers must still ensure necessity and transparency. [Recognised legitimate interests under DUAA]

Appendix 4: Subject access requests (quick reference)

• Verify identity/authority;

• Clarify scope if needed;

• “Stop the clock” applies while awaiting ID/clarification;

• Conduct reasonable and proportionate searches;

• Respond within one month of receiving necessary information (extend by two months if complex);

• Apply exemptions carefully;

• Keep an audit trail. [DUAA SARs: reasonable/proportionate and stop-the-clock]