Data Protection Policy

KINGSLEY

Reviewed: October 2026
Next Review: October 2027

Introduction

This Data Protection Policy has been produced to ensure compliance with the Data Protection Act 2018 (the DPA 2018, the UK General Data Protection Regulation (UK GDPR) and all associated legislation.

The DPA 2018 gives individuals rights over their personal data and protects individuals from the erroneous use of their personal data.

In light of the enactment of the Data (Use and Access) Act 2025 (DUAA), this policy has been updated to reflect the amended UK GDPR and Data Protection Act 2018 regime, preserving core privacy protections while enabling responsible data use under DUAA's new flexibilities

Kingsley Primary School is the data controller for the personal data it processes about individuals and pays the data protection fee to the Information Commissioner's Office (ICO). Its registration number is [Z6036245]

The school has an appointed Data Protection Officer to:

- Inform and advise the school and its staff about their obligations to comply with the UK GDPR and other data protection laws.

- Monitor the school's compliance with the UK GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits and providing the required training to staff members.

- The DPO reports to the highest level of management at the school, which is the Governing Board and the Headteacher. The DPO acts independently and is given the resources needed to carry out the role.

- Our data protection officer is provided by ADNS Group and can be contacted at the following address:

5 Eggleston Court, Riverside Park

Middlesbrough

TS2 1RU

Tel No: 01642 248750

Email: compliance@adnsgroup.com

Purpose

This policy supports the school's compliance with the UK GDPR, the DPA 2018 and the DUAA 2025. The policy outlines our overall approach to its responsibilities and legal obligations as the 'Data controller' under all legislation.

Scope

This policy applies to all employees (including temporary, casual or staff), governors, volunteers, contractors and consultants working for or on behalf of the school. It also applies to any service providers that we contract with who process personal information on behalf of the school.

This policy also covers any staff who may be involved in research or other activity that requires them to process or have access to personal data, for instance as part of research or as part of a professional practice activities. If this occurs, it is the responsibility of the school to ensure the data is processed in accordance with the current legislation and that pupils and staff are advised about their responsibilities.

Data covered by the policy

Personal data is any information relating to an identified or identifiable living individual, such as a name, address, photograph, assessment result or identification number. Further guidance is available from the ICO. This includes data held manually and electronically and data compiled, stored, or otherwise processed by us or by a third party on its behalf.

Special category data is personal data consisting of information relating to:

- Racial or ethnic origin
- Political opinions, religious or philosophical beliefs
- Membership of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)
- Physical or mental health or condition
- Sex life or sexual orientation
- Genetic data
- Biometric data used to identify an individual (for example, fingerprints used for cashless catering)

Criminal offence data (information about criminal allegations, proceedings or convictions, including information from DBS checks) is given similar protection and may only be processed where the law allows it.

The seven data protection principles

The UK GDPR requires the school, including staff, governors and other individuals who process personal information on its behalf, to comply with the seven data protection principles. Personal data must:

- Be processed lawfully, fairly and in a transparent manner.
- Be collected for specified, explicit and legitimate purposes and not processed in a manner incompatible with that purpose.
- Be adequate, relevant and limited to what is necessary for the purposes for which it is being collected.
- Be accurate and kept up to date.
- Not be kept for longer than is necessary for the purpose.
- Be kept safe from unauthorised or unlawful processing and against accidental loss, destruction, or damage.
- Be processed in a way that allows the school to demonstrate its compliance with these principles (accountability).

All new members of staff will be required to complete a mandatory information governance module as part of their induction and existing staff will be requested to undertake refresher training on a regular/annual basis.

Employees within the School are expected to:

- Familiarise themselves and comply with the seven data protection principles
- Ensure any possession of personal data is accurate and up to date
- Ensure their own personal information is accurate and up to date
- Keep personal data for no longer than is necessary.
- Ensure that any personal data they process is secure and in compliance with the school's information security and related policies.
- Acknowledge data subjects' rights e.g. the right of access to their personal data held by the school) and pass any request from an individual about their data to the School Business Manager on the day it is received.
- Ensure personal data is only used for those specified purposes and is not unlawfully used for any other purpose.
- Ensure there is a lawful basis before collecting, sharing or disclosing personal data (see 'Lawful basis for processing' below). Consent should only be used where the school has decided it is the appropriate basis, for example for publishing pupil photographs.

Employees can contact the DPO at compliance@adnsgroup.com if they require advice or guidance, need to report data protection breach, or have any concerns relating to the processing of personal data under the DPA 2018.

Lawful basis for processing

The school may only process personal data where it has a lawful basis under Article 6 of the UK GDPR. Most of the school's processing is necessary to carry out its public task of providing education (including safeguarding) or to comply with a legal obligation, such as the school census, attendance registers and pre-employment checks. Some processing is necessary for a contract, such as an employment contract, or to protect someone's vital interests in an emergency.

Consent is only used where individuals have a genuine choice, for example the use of pupil photographs on the school website or social media, and the use of biometric data. Consent is recorded and can be withdrawn at any time. Because of the imbalance of power, the school does not rely on consent to process staff data as part of their employment.

Special category data may only be processed where a condition under Article 9 of the UK GDPR, and where required Schedule 1 of the DPA 2018, also applies – for example employment obligations, the safeguarding of children and individuals at risk, or health and social care. Criminal offence data, such as DBS check information, is only processed where the DPA 2018 allows it. The school maintains an Appropriate Policy Document for this processing.

Photographs, CCTV and biometric data

The school will ask for consent before using images of pupils for publicity, including the website, social media, newsletters and the press, and will not publish a pupil's full name alongside their image without specific consent. Parents may take photographs at school events for their own family use but are asked not to share images of other children online.

Records Management and Responsibilities

Kingsley Primary School must manage its records and record-keeping systems in compliance with applicable regulations, including the Data (Use and Access) Act 2025. This legislation updates UK GDPR, Data Protection Act 2018, and PECR.

The Governing Body has overall accountability for data protection and approves this policy. The Headteacher and Facilities Manager are responsible for its day-to-day implementation, with advice from the Data Protection Officer (DPO). School Business Manager serves as the accountable champion: overseeing policy and strategy, ensuring resources are allocated, and triggering remediation when issues arise. They'll provide guidance on records management best practices, ensuring information is accurate, readily retrievable, and managed securely and promptly. Compliance will be monitored through an annual review to verify secure storage and appropriate access. They'll also advocate for resources and training under the enhanced requirements introduced by the 2025 Act.

More information can be found in the school's retention schedule.

Obtaining, disclosing, and sharing

Only personal data that is necessary for a specific purpose should be obtained.

The school will tell pupils, parents, staff and others how their information will be used through its privacy notices, which are published on the school website.

Staff personal data is processed because it is necessary for their employment contract and to meet the school's legal obligations, as explained in the workforce privacy notice.

Data must be collected and stored in a secure manner. Personal information must not be disclosed to a third-party organisation without prior consent of the individual concerned unless the disclosure is legally required or permitted. This also includes information that would confirm whether an individual is or has been an applicant, pupil or employee of the school.

Kingsley Primary School may have a duty to disclose personal information to comply with legal or statutory obligation. Data protection law may permit the school to share data without consent or without informing individuals in accordance with the right to be informed:

1. With the police and law enforcement bodies where it is considered necessary for the prevention and detection of crime.
2. Where the information may be necessary under enactment, for the purposes of legal proceedings and or for exercising of defending legal rights.
3. Where the processing is necessary because it is a task carried out in the public interest, for example sharing information with the local authority for safeguarding and child protection.

Data protection law does not prevent the sharing of information where this is necessary to keep a child safe. In line with Keeping Children Safe in Education, staff must share safeguarding concerns with the Designated Safeguarding Lead without delay.

All requests from third party organisations seeking access, to personal data held by us should be directed to the school office and/or the Data Protection Officer at compliance@adnsgroup.com. We will keep a record of all requests received from third party organisations. This information may be requested by the DPO or the information commissioner at any time to comply and actively evidence compliance, with data subject rights.

Personal information that is shared with third parties on a more regular basis shall be carried out under written agreement to stipulate the purview and boundaries of sharing. For circumstances where personal information would need to be shared in the case of ad hoc arrangements, sharing shall be undertaken in compliance with the DPA 2018. Organisations that process personal data on the school's behalf must do so under a written contract that meets Article 28 of the UK GDPR. Personal data will only be transferred outside the UK where the requirements of the UK GDPR are met, and the DPO should be consulted first.

Retention, security, and disposal

Recipients responsible for the processing and management of personal data need to ensure that the data is accurate and up to date. If a pupil, parent, member of staff or applicant is dissatisfied with the accuracy of their personal data, then they must inform the Headteacher or Facilities Manager.

Personal information held in paper and electronic format shall not be retained for longer than is necessary. In accordance with data protection principles of the DPA 2018, personal information shall be collected and retained only for business, regulatory or legal purposes.

In accordance with the provisions of the DPA 2018, all staff whose work involves processing personal data, whether in electronic or paper format must take personal responsibility for its secure storage and ensure appropriate measures are in place to prevent accidental loss or destruction of or damage to personal data. Staff working from home will be responsible for ensuring that personal data is stored securely and is not accessible to others.

All departments should ensure that data is destroyed in accordance with the retention schedule when it is no longer required. Personal data in paper format must be cross-cut shredded or placed in the school's confidential waste. Personal data in electronic format should be deleted. Hardware and storage media must be securely wiped or destroyed by the school's approved IT provider, and a certificate of destruction obtained and retained.

Transferring personal data

Any transfer of personal data must be done securely in line with the school's information security and acceptable use policies. Email communication is not always secure and sending personal data via external email should be avoided unless it is encrypted with a password provided to the recipient by separate means such as via telephone.

Care should be taken to ensure emails containing personal data are not sent to unintended recipients. It is important that emails are addressed correctly, and care is taken when using reply all or forwarding or copying others into emails. Use of the blind copy facility should be considered when sending an email to multiple recipients to avoid disclosing personal information to others.

Personal email accounts should not be used to send or receive personal data for work purpose.

Data subjects' rights and subject access requests

Under the UK GDPR and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025 (DUAA), individuals have the following rights, some of which apply only in certain circumstances:

- Be informed about how their personal data is used, through the school's privacy notices.
- Access to personal information processed by the school.
- Object to processing of their personal data, including processing carried out in the public interest.
- Prevent processing for direct marketing.
- Not be subject to significant decisions based solely on automated processing without safeguards, including the right to human intervention and to contest the decision.

- In certain circumstances, have inaccurate or incomplete personal data rectified, restricted or erased.
- Receive personal data they have provided in a portable format, where processing is based on consent or contract and carried out by automated means.
- Withdraw consent at any time, where processing is based on consent.
- Complain to the school and to the Information Commissioner's Office (ICO).

Individuals can make a 'subject access request' (SAR) to any member of school staff, verbally or in writing, to request access to personal information the school holds about them, subject to any exemptions or restrictions that may apply. The school shall use its discretion under the DPA 2018 and DUAA to encourage informal access at a local level to a data subject's personal information, but the school's formal procedure for processing SARs must be followed to comply with legislation.

Any individual who wishes to exercise their right of access can do so verbally or in writing. The school will not normally charge a fee, but may charge a reasonable fee, or refuse to respond, where a request is manifestly unfounded or excessive. The school may offer a form to help, but will not require one to be used. Where there is reasonable doubt about the identity of the requester, or their authority to act on behalf of the data subject, the school will ask for proof before releasing information.

The requested information will be provided within the statutory timescale of one month from receipt of the request. Where clarification is required, the statutory timeframe will be paused ("stop the clock") until the requested information is provided. In cases of complex or multiple requests, the school may extend the timeframe by up to two additional months, notifying the individual within the original one-month period and explaining the reason for the extension.

Under DUAA, the school will conduct reasonable and proportionate searches to locate requested information. The school will not be required to search every system or archive where this would be disproportionate. Information subject to legal privilege or other statutory exemptions will not be disclosed.

Personal data about a child belongs to that child. Parents may make a request on behalf of a child who is not mature enough to understand their rights, or where the child has given permission. Children aged 12 and over are generally considered mature enough to make their own requests, but each case is considered individually and in the child's best interests.

Parents also have a separate right to access their child's educational record under the Education (Pupil Information) (England) Regulations 2005. The school will respond within 15 school days.

Data protection complaints

The school maintains a formal internal complaints process for all data protection complaints, not only those about SARs.

Complaints can be made in writing, by email to the school office email address. All complaints will be acknowledged within 30 days, investigated without undue delay, with updates provided throughout and the outcome communicated without undue delay. Individuals retain the right to escalate complaints to the Information Commissioner's Office (ICO) if dissatisfied (www.ico.org.uk, telephone 0303 123 1113).

Reporting a data security breach

We are legally required to notify the ICO of any data breach that is likely to result in a risk to individuals' rights and freedoms, without undue delay and within 72 hours of becoming aware of it, in accordance with the Data Protection Act and the Data (Use and Access) Act 2025. All breaches—regardless of size must be reported internally and managed in line with this policy and the school's data breach procedure. Failure

to comply may result in fines or enforcement action by the ICO. Where appropriate, additional training will be provided to employees involved, based on severity and recurrence.

All breaches, whether minor or significant, must be reported immediately to the Data Protection Officer (DPO) at ADNS Group (contact: 01642 248750). The DPO will investigate the incident within 24 hours and record it in the breach register, even if no harm occurred.

Following the initial investigation, the DPO will assess the severity of the breach and inform senior management. If necessary, legal advice will be sought. This assessment will be completed within 24 hours of breach awareness.

The DPO and Administration Manager will develop a recovery plan to minimise risks. Interviews with involved individuals will identify root causes and corrective measures within 24 hours of the assessment.

If the breach is likely to result in a risk to individuals' rights and freedoms, the ICO will be notified without undue delay and within 72 hours of the school becoming aware of it. Where it is likely to result in a high risk, affected individuals will also be informed without undue delay. Notifications to the ICO will include:

- Details of the breach (what happened, how, and when it was discovered)
- The categories and approximate number of individuals and records affected
- The likely consequences of the breach
- Actions taken in response
- Contact details of the DPO

Affected individuals will receive clear and transparent communication. Depending on severity, relevant third parties—such as the police, the local authority or insurers, will also be notified within five days of breach awareness.

Monitoring and review

This policy will be reviewed annually by the Administration Manager and the DPO, or sooner if the law or guidance changes, and approved by the Governing Body.