

Privacy notice for pupils

Kings Academy Trust

**Effective from**

1 September 2026

Next review

September 2027, or earlier if processing changes

Contents

- 1. Introduction
- 2. Personal information we use
- 3. Why we use it
- 4. Lawful bases
- 5. Special category and criminal offence data
- 6. How we collect information
- 7. Retention and security
- 8. Sharing and international transfers
- 9. Your data protection rights
- 10. Automated decision-making and profiling
- 11. Data protection complaints
- 12. Contact us

1. Introduction

This privacy notice explains how Kings Academy Trust collects and uses personal information about children and young people who attend a Kings Academy Trust academy, including former pupils where records are retained. It applies across the Trust and its academies unless a more specific notice is provided at the point of collection.

Kings Academy Trust is the data controller. We process personal information under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and the Data (Use and Access) Act 2025.

The Trust's Data Protection Officer is Satswana and can be contacted at admin@satswana.com.

A quick guide for pupils

We use information about you so we can teach and support you, keep you and other people safe, run the academy and meet the law. We only use information we need, protect it carefully and keep it for no longer than necessary.

You can ask what information we have about you, tell us if something is wrong and ask questions about how it is used. Depending on your age and understanding, you may exercise your rights yourself or with help from a parent or carer. Contact details are in section 12.

2. Personal information we use

- personal identifiers and contacts, such as name, preferred name, date of birth, address, unique pupil number, pupil photograph and emergency contacts
- characteristics, such as sex, ethnicity, language, nationality, country of birth, religion and eligibility for free school meals or other support
- family, admissions, previous-school and educational-history information
- attendance, absence, punctuality, exclusions, suspensions and alternative-provision information
- curriculum, class, assessment, attainment, examination, destination and careers information
- special educational needs and disabilities, education health and care plans, support and access arrangements
- medical, allergy, dietary, medication, first-aid, accident and healthcare information
- pastoral, wellbeing, behaviour, safeguarding, child-protection and professional-involvement records
- information about looked-after or previously looked-after status where applicable
- school meal, trip, club, transport, library, equipment and payment records
- work created by pupils, photographs, video, audio and CCTV images
- accounts and activity on academy devices, networks, email, learning platforms and other digital services, including filtering, monitoring, access and security logs
- biometric information, only where an academy uses an approved biometric system and the required consent has been obtained
- information about complaints, incidents, insurance matters or legal claims.

3. Why we use it

- admit pupils and organise teaching, timetables, examinations and learning support
- support learning and monitor and report on progress, attainment and destinations
- record and improve attendance and manage behaviour, suspensions, exclusions and alternative provision
- identify and meet special educational, disability, medical, pastoral and accessibility needs
- safeguard pupils, promote wellbeing and provide appropriate care and support
- communicate with pupils, parents and carers and manage meals, trips, clubs, transport, payments and other academy services
- provide and protect accounts, devices, networks and online services, including safeguarding filtering and monitoring
- celebrate achievement and communicate about academy life where publication is lawful
- assess service quality, plan resources, allocate funding and support research and statistics
- meet statutory education data collections and other legal, regulatory, inspection, audit and safeguarding duties.

4. Lawful bases

We select the lawful basis that applies to each purpose. The principal bases are:

- Article 6(1)(c), legal obligation: processing required by education, attendance, safeguarding, equality, health and safety, examination, funding and other laws
- Article 6(1)(e), public task: processing necessary to provide education, safeguard children and carry out the Trust's official functions where those functions have a clear basis in law
- Article 6(1)(d), vital interests: processing necessary to protect someone's life
- Article 6(1)(b), contract: limited processing for an optional service where the pupil is a party to a contract or asks us to take steps before entering into one
- Article 6(1)(f), legitimate interests: organisational security, fraud prevention, legal claims and other non-statutory activity where this is not an official public task and the pupil's interests and rights do not override the interest
- Article 6(1)(a), consent: genuinely optional uses, such as certain publicity images or non-essential activities. Consent may be withdrawn at any time.

The underlying legal framework includes, where applicable, the Education Acts, Education (Information About Individual Pupils) (England) Regulations 2013, Education (Pupil Registration) (England) Regulations, Children Acts, Equality Act 2010, UK safeguarding law and statutory guidance, examination regulations and the Trust's academy funding arrangements.

5. Special category and criminal offence data

Some information needs additional protection under data protection law. The special category data we may use includes:

- racial or ethnic origin, religious or philosophical beliefs and information about sex life or sexual orientation where relevant to safeguarding, support or equality
- health, disability, special educational needs and medical information
- genetic information or biometric information used for unique identification, where applicable.

We use this information only where it is necessary for the purposes described in this notice and where we have both an Article 6 lawful basis and an Article 9 condition. Depending on the purpose, the Article 9 conditions we rely on are:

- Article 9(2)(g): substantial public interest supported by an applicable DPA 2018 Schedule 1 condition, including safeguarding children, equality of opportunity, preventing unlawful acts and protecting the public
- Article 9(2)(h): health or social-care purposes where the required professional or legal confidentiality safeguards apply
- Article 9(2)(b): social-protection obligations and rights where applicable
- Article 9(2)(f): establishing, exercising or defending legal claims
- Article 9(2)(j): archiving, research or statistical purposes with the required safeguards
- Article 9(2)(a): explicit consent where it is appropriate and freely given.

Photographs and ordinary CCTV images are personal data but are not automatically special category data. They become biometric special category data only if they are technically processed to uniquely identify a person.

Where we use information about criminal convictions or offences, including relevant DBS information, we do so under Article 10 UK GDPR and an applicable condition in Schedule 1 of the Data Protection Act 2018. This will normally relate to employment, safeguarding, preventing fraud or protecting children and other vulnerable people. Where required, the Trust maintains an Appropriate Policy Document.

Biometric information

If an academy proposes to use a pupil's biometric information for identification—for example, for cashless catering—it will provide specific information first and follow the Protection of Freedoms Act 2012. Written parental consent will be obtained for pupils under 18, and the pupil may object or refuse at any time. A reasonable alternative will be provided. This section does not mean that every academy uses biometric systems.

6. How we collect information

We collect information from pupils and parents or carers through admissions and annual-update forms, classroom and assessment activity, attendance and safeguarding processes, academy systems, devices, platforms, examinations, trips, clubs, catering and routine communications. We will explain whether information is mandatory or voluntary when it is requested.

We may also receive information from previous or other schools, the Department for Education, local authorities, examination and assessment bodies, health and social-care professionals, safeguarding partners, police, courts, youth-support and careers services, alternative-provision providers and contracted service providers.

When we receive information from another source, we provide privacy information within the period required by law unless an exemption applies or the pupil already has the relevant information.

7. Retention and security

We keep pupil information while the pupil attends a Trust academy and afterwards for the periods set out in the Data Retention Schedule.

The exact period depends on the type of record. We apply the Trust's Data Retention Schedule, taking account of statutory record-keeping duties, safeguarding requirements, financial and audit rules, limitation periods, regulatory guidance and whether information is needed to establish, exercise or defend legal claims. Different periods apply to the pupil record, admissions, attendance, attainment, examinations, safeguarding, SEND, medical, behaviour, trips, payments, photographs, CCTV and digital-system logs. Safeguarding and certain educational records may need to be retained for considerably longer than routine administrative records.

We use appropriate technical and organisational measures to protect personal information against accidental loss, unauthorised access, alteration or disclosure. Access is limited to people who need the information for their role. Information is securely deleted or destroyed when it is no longer required.

A copy of the relevant retention schedule or further information about a particular retention period is available from the Data Protection Officer.

8. Sharing and international transfers

Where necessary and lawful, we may share pupil information with:

- parents or carers, taking account of the pupil's age, understanding, safety and rights
- schools, colleges, alternative-provision settings and other education providers
- the Department for Education, local authorities, Ofsted and other education or funding bodies
- examination boards, assessment organisations, careers and destination services
- health, social-care, safeguarding, youth-support and emergency services
- police, courts and other bodies with lawful information-gathering powers
- catering, payment, transport, communications, learning-platform, IT, filtering, monitoring, records-management and security providers
- auditors, insurers, professional advisers, researchers and organisations providing pupil or family support.

We do not share pupil information simply because someone asks for it. We check that sharing is necessary, proportionate and supported by a lawful basis or that valid consent has been given.

Department for Education data collections

The Department for Education collects pupil information from education settings and local authorities through statutory data collections. As an academy trust, we are required to share pupil information for the school census and other applicable collections under regulation 5 of the Education (Information About Individual Pupils) (England) Regulations 2013.

This information supports school funding, education policy, accountability, research and statistics. Data is transferred securely. Information about collection requirements is available at <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.

The National Pupil Database

Information submitted to the Department for Education may be stored in the National Pupil Database (NPD). The NPD is used for education funding, policy, accountability, research and statistical purposes. The Department for Education may share data from the NPD only where it considers the sharing lawful, secure and ethical and its approval controls are met.

Further information is available at <https://www.gov.uk/government/publications/national-pupil-database-npd-privacy-notice> and in the Department for Education privacy information for learners at <https://www.gov.uk/government/publications/privacy-information-early-years-foundation-stage-to-key-stage-3> and <https://www.gov.uk/government/publications/privacy-information-key-stage-4-and-5-and-adult-education>.

Youth-support and careers services

For pupils aged 13 and over, we may share limited information with the local authority or its youth-support provider so it can meet responsibilities for the education or training of young people under section 507B of the Education Act 1996. This normally includes name, address and date of birth. Additional information is shared only where the law permits or valid consent is provided. At age 16, relevant choices about additional sharing transfer to the young person.

International transfers

Some service providers may store or allow access to personal information outside the UK. Before making a restricted transfer, we check that UK adequacy regulations apply, or put in place an appropriate safeguard such as the UK International Data Transfer Agreement or UK Addendum and complete the required data protection test. We use an Article 49 exception only where the law permits. Contact the Data Protection Officer for information about the safeguard used for a particular service.

9. Your data protection rights

Depending on the circumstances and the lawful basis being used, you may have the right to:

- be informed about how we use your personal information
- ask for access to the personal information we hold about you
- ask us to correct inaccurate or incomplete information
- ask us to erase information or restrict its use in certain circumstances
- object to processing in certain circumstances, including direct marketing
- receive information in a portable format where the right to data portability applies
- withdraw consent at any time where consent is our lawful basis, without affecting earlier lawful processing
- ask for safeguards and human involvement where a significant decision is made solely by automated means
- complain to us and to the Information Commissioner's Office.

These rights are not absolute. For example, erasure does not normally apply where we must keep information to comply with a legal obligation or perform a public task. We will explain any restriction that applies when responding to a request.

To exercise a right, contact the Data Protection Officer or the Trust's Data Protection Lead using the details in section 12. We may ask for information needed to confirm identity and locate the relevant records.

Children have the same data protection rights as adults. A pupil who has sufficient understanding may exercise these rights personally. A parent or carer may help the pupil or act on their behalf where appropriate, but parental responsibility does not automatically give unrestricted access to all of a child's personal information.

A parent or carer may also ask to see a child's educational record. The academy will consider the request under the education law that applies to the academy and in a way that respects the pupil's data protection rights and safeguarding needs.

10. Automated decision-making and profiling

The Trust does not currently make decisions about you based solely on automated processing where the decision has a legal or similarly significant effect. Digital and artificial-intelligence tools may support administrative work, but accountable staff remain responsible for significant decisions.

If this changes, we will update the relevant privacy information before the processing begins and explain the logic involved, likely effects and safeguards, including how to obtain human intervention and challenge a decision.

Filtering and monitoring systems may automatically analyse network or device activity to identify security or safeguarding risks. Alerts are reviewed by authorised staff; the systems are not used to make solely automated decisions about pupils with legal or similarly significant effects.

11. Data protection complaints

You can make a data protection complaint by emailing admin@satswana.com or ddonnelly@kingsacademytrust.co.uk, or by writing to the Trust at the address in section 12. Please describe the issue and the outcome you are seeking.

We will acknowledge receipt within 30 days. Without undue delay, we will make appropriate enquiries, keep you informed where an investigation is continuing, and tell you the outcome and any action taken.

You may also complain to the Information Commissioner's Office. The ICO can be contacted on 0303 123 1113 or through <https://ico.org.uk/make-a-complaint/>. The ICO's postal address is Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

12. Contact us

Kings Academy Trust, City Approach 1, Albert Street, Eccles, M30 0BG

Data Protection Officer: Satswana — admin@satswana.com

Data Protection Lead: David Donnelly — ddonnelly@kingsacademytrust.co.uk