

Privacy notice for visitors

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 visitors to Trust and academy premises, including invited guests, contractors, professionals and event attendees. 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.

2. Personal information we use

- name, contact details, organisation, host and purpose of visit
- arrival and departure times, visitor-pass details, signature and vehicle registration
- identity, safeguarding, DBS or professional-status evidence where appropriate to the visit
- health, emergency, accessibility or evacuation information where needed
- photographs, CCTV images and access-control or security logs
- information about incidents, accidents, safeguarding concerns or alleged misconduct connected with a visit
- network or guest-system use where access is provided.

3. Why we use it

- manage visits, verify identity and contact hosts
- safeguard pupils and protect visitors, staff, premises and property
- support emergency evacuation, first aid, incident response and investigations
- provide accessibility arrangements
- meet health and safety, safeguarding, insurance and regulatory requirements
- administer contracted work or services where applicable.

4. Lawful bases

- Article 6(1)(c), legal obligation: health and safety, safeguarding and other legal requirements
- Article 6(1)(e), public task: visitor processing necessary to safeguard pupils and operate the Trust's education functions
- Article 6(1)(b), contract: where the visit is necessary to enter into or perform a contract with you
- Article 6(1)(f), legitimate interests: premises security, fraud prevention and efficient visit administration where this is not an official public task and your rights do not override the interest
- Article 6(1)(d), vital interests: responding to a life-threatening emergency
- Article 6(1)(a), consent: genuinely optional uses such as particular publicity photographs.

5. Special category and criminal offence data

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

- health, disability and accessibility information provided for safety or reasonable adjustments.

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
- Article 9(2)(h): health or social-care purposes subject to the required safeguards
- Article 9(2)(f): establishing, exercising or defending legal claims
- Article 9(2)(a): explicit consent where appropriate.

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.

6. How we collect information

We collect information from you when a visit is arranged, when you sign in, while you are on site and when an incident or enquiry occurs. Some information is mandatory for site access; if it is not provided, entry may be refused or additional supervision may be required.

We may also receive information from your organisation, the person hosting you, a contractor or event organiser, the relevant academy, a sign-in or security provider, safeguarding partners, police or emergency services.

7. Retention and security

Visitor information is retained only for the period needed for site management, safeguarding, health and safety, security, insurance and legal purposes, in accordance with the Data Retention Schedule and relevant CCTV arrangements.

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. Routine visitor logs and CCTV are generally kept for shorter periods than records linked to an accident, safeguarding concern, security incident, contract or legal claim. We do not normally retain a copy of a DBS certificate.

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 visitor information with the relevant academy and Trust staff, your organisation or host, sign-in and security providers, IT support, local authorities, safeguarding partners, emergency services, police, Ofsted, insurers, professional advisers, courts and regulators.

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.

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.

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