

Privacy and Data Policy

 Last updated 5 January 2026

This Privacy and Data Policy outlines how Public Sector Analytics Ltd t/a askKira, a Limited Company registered in England and Wales (Company Number: 14889377) operating in the field of education technology, collects, uses, processes and safeguards data from users of our AI chatbot for organisations – askKira.com. We are committed to maintaining the privacy and security of your personal information.

Introduction and Overview

Our Role as Data Controller or Processor

Depending on how you use askKira, Public Sector Analytics Ltd t/a askKira may act as either a data controller or a data processor.

- If your organisation (e.g. school, trust or institution) provides access, askKira acts as a data processor, processing personal data solely on behalf of the organisation and in accordance with their instructions, as outlined in the Order Form.
- If you sign up as an individual, askKira acts as the data controller of your personal data. In this case, we determine the purpose and means of processing your data, in line with this Privacy and Data Policy.

This policy applies to both types of user. Where relevant, we explain which terms apply depending on how you access our services.

Consent

As an individual using our AI educational chatbot, you consent to the collection and processing of your data as described in this policy. You can withdraw your consent at any time by discontinuing use of our services. You can also opt-out of marketing from askKira by clicking Unsubscribe at the bottom of any of our emails, declining cookies on our website or by completing this form.

Where your organisation signs up for askKira, consent is managed at the organisational level. Where you are an individual user, you may withdraw consent at any time.

Data Collection and Usage

Types of Data Collected

We collect user information such as name, email address, educational background and professional interests, as well as interactions and queries made with the AI chatbot. Additionally, we collect specific personal information including name, email address, job title and date of birth. This information is collected for the purpose of generating user accounts and enabling personalisation of our services.

Purpose of Data Collection

Your data is collected when you engage with our chatbot, subscribe to our services, download resources or contact us for support. This engagement allows us to gather the information necessary to provide you with our services and support. As you interact with our services, we automatically collect data regarding your device and usage patterns through cookies and similar technologies. This data enhances our service's functionality and user experience.

Additionally, we utilise your demographic data for marketing purposes, such as sending email newsletters to keep you updated on our latest products, services and industry insights.

We may fine-tune or train our AI models with our own proprietary inputs to enhance its utility and relevance to our users. This process is part of our commitment to providing a service that is responsive to the needs of our user base. We do not use user inputted data for fine-tuning or training our AI models.

The chat history feature is powered by a secure database that stores key-value pairs, linking a user ID to their submitted queries and responses. These records are accessible only to the individual user whose unique key matches the stored entry.

No Training or Sharing of User Data

No user-submitted data is used to train any language models, nor is it shared externally or made viewable by any third party, nor is any data passed into a system that would retain it outside the secured infrastructure.

Data Processing and Sharing

Data Processing

Public Sector Analytics Ltd (t/a askKira) enters into Data Processing Agreements (DPA) with all third-party service providers and external consultants who process anonymised data on our behalf. These agreements ensure that data is processed in compliance with UK GDPR, upholding stringent data protection and privacy standards.

Anonymised data is processed by our business intelligence platform and external consultants, under separate DPAs, to provision the Public Sector Analytics insights offering. This processing is conducted based on clients' opted-in selection in their order form for anonymised usage and

behavioural analytics and is used to generate insight and intelligence reports. The DPA governs how data processors handle the data, including maintaining confidentiality, ensuring data security and adhering to the specified processing purposes. All processors are subject to regular audits to ensure ongoing compliance with these obligations.

Organisational users should contact their school or trust to make requests under UK GDPR and we will assist the organisation as required. If you are an individual user, you may contact us directly for any data rights requests at info@askkira.com.

All data entered into the platform either through account set up or user input is processed in real time to generate responses, after which it is only stored for user-facing features (such as saved conversations, account profile data or automatic organisational insights). We apply a privacy-by-design approach, meaning we collect the minimum data required to deliver the service.

Formal Data Processing Agreement

A formal Data Processing Agreement can be issued for signing as part of your contract with us.

Data Sharing

We anonymise user data for analytics to understand service usage and improve educational outcomes. This approach ensures privacy while contributing valuable insights to the educational leaders. No raw or identifiable data shall be shared externally under any circumstances. No data from the platform is sold or shared with third-party products or services, either directly or through partnerships. askKira does not sell, share or transfer any user-submitted data to third-party products or services – either directly or through partnerships.

Public Sector Analytics Insights Dashboard

Public Sector Analytics provides an insights dashboard that shares anonymised usage and behavioural insights from across all of an organisation's askKira userbase. This dashboard informs a school of their users' behaviours benchmarked and compared to other similar organisations' userbase. It's important to note that no personal data is processed for the provision of this insights dashboard. All data used to generate insights has any identifiable traits or markers removed. We also implement a minimum sample size to generate insights to avoid bias and exposure.

Organisational users can opt-in to the Public Sector Analytics insights offering via the order form. This opt-in allows us to process anonymised usage and behavioural analytics data for the purpose of generating insight and intelligence reports, which are only visible to the Organisation themselves.

Third Party Services and Processing

We may engage third-party service providers to assist with data analysis and storage, but we ensure that they adhere to strict privacy and security standards. Our service providers include:

- **Amazon Web Services** – Provides secure cloud hosting and infrastructure to ensure the reliability and scalability of our platform.
- **Microsoft Azure** – Supports certain AI powered functionalities and secure data storage.
- **OpenAI** – Used for certain AI-powered functionalities. OpenAI does not use API data for training models, though it may temporarily log data for abuse prevention.
- **Google** – Includes Google Analytics for understanding website traffic and user interactions, as well as the Gemini model for AI-powered functionalities. Google does not use API data from Gemini for training their models.
- **Anthropic** – Used for AI-powered functionalities via the Claude model. Anthropic does not use API data for training their models.
- **Perplexity** – Used for certain AI-powered functionalities. Perplexity does not use API data for training their models.
- **Hotjar** – Provides heatmaps and behavioural analytics to optimise user experience. No personally identifiable information is collected.
- **Stripe** – Processes secure online payments. Stripe follows strict financial security protocols and does not share payment details with unauthorised third parties.
- **Mailchimp** – Manages our email communications. Subscribers can opt out at any time, and no data is shared beyond its intended use.
- **Wonde** – Securely connects with education platforms to enable data access while maintaining strict compliance with GDPR and other data protection laws.
- **Cloudflare** – Provides security and performance enhancements, including DDoS protection and traffic optimisation. No personal data is sold or shared.

We ensure that all our service providers comply with relevant data protection regulations, including GDPR and UK data protection laws. If we change or add a sub-processor, we will notify all users within a reasonable timeframe.

Data Security and Hosting

Our services are hosted on Amazon Web Services (AWS), with data stored primarily in the United Kingdom (London region). Some ancillary services may store or process data within the EEA. All transfers are subject to UK GDPR-compliant safeguards.

Our Information Security Policy includes:

- **Access Control:** Only authorised personnel have access to sensitive and anonymised data, with access granted strictly on a case by case and need-to-know basis.
- **Encryption:** All sensitive data is encrypted both in transit and at rest to protect against unauthorised access.

- **Monitoring and Auditing:** We continuously monitor our systems for vulnerabilities and conduct regular audits to ensure compliance with our security policies.
- **Incident Response:** In the event of a security breach, we have a well-defined incident response plan to mitigate damage, notify affected parties and resolve the issue efficiently.
- **Training:** All employees and contractors undergo regular security awareness training to ensure they understand their responsibilities in protecting sensitive data.

Data Breach Notification

In the event of a data breach, we are committed to notifying affected users and relevant authorities as soon as possible after becoming aware of the breach, and no later than 72 hours after discovery. We have procedures in place to detect, report and investigate suspected data breaches promptly.

Where we act as a processor on behalf of an organisation, we will inform the relevant data controller without undue delay, enabling them to notify the ICO and affected individuals if required. Where we act as a controller (e.g. for individual user data), we will notify affected users and the ICO within required timeframes and take all necessary steps to contain, report and resolve the incident.

Risk Assessment Strategy

Public Sector Analytics Ltd employs a comprehensive Risk Assessment Strategy to identify, evaluate and mitigate potential risks to data security and privacy. This strategy includes regular risk assessments, mitigation plans, ongoing reviews and compliance monitoring closely aligned with UK GDPR.

Cookies and Tracking

We use cookies and similar technologies to enhance your user experience, gather usage data for analytical purposes and for marketing initiatives. By using our AI educational chatbot, you consent to analytics tracking via Google, Hotjar and X to help us understand user behaviour, improve our services and provide personalised content and advertisements. You can manage your cookie preferences through your browser settings.

Data Retention

We retain personal data only for as long as necessary to deliver services and meet contractual or legal obligations. Chat history is stored solely to enable users to review past interactions and remains available unless deleted manually, by the organisation, or via an automatic deletion setting.

For individual users, personal data is retained only while the account is active and is deleted upon account closure or user request. For organisational users, data is retained for the duration of the contract and up to 12 months thereafter for compliance or audit purposes. All data will then be

securely deleted or returned as instructed by the organisation. No user submitted data is retained for training purposes and chat history can be deleted on request.

User Rights and Legal Information

Access and Correction: You have the right to access, correct, delete and restrict processing of your personal data in accordance with UK GDPR.

Erasure: You can request the deletion of your data, and we will comply within a reasonable timeframe. Users can delete their own chat history via the interface. If administrators require content to be deleted at an organisational level, we can action this on request. This deletion is permanent.

Data Subject Access Request Process: To request access to your personal data, contact our Data Protection Officer at info@askkira.com. We aim to respond to all legitimate requests within a reasonable timeframe. There is no fee for making a request unless the request is clearly unfounded, repetitive or excessive.

Intellectual Property Rights

There is no transfer of intellectual property when content is submitted to askKira. The interaction is best understood as akin to a teacher reading a piece of work — in this case, the review is done by a model rather than a person. askKira processes user-submitted content solely for the purpose of generating a one-time AI-powered response. No content is retained or reused beyond that session unless required to provide a specific feature (e.g. saved chat history). Ownership of submitted content remains with the user or Organisation, and no IP rights are transferred to us. The original author or organisation retains full rights over any content submitted to the platform, including pupils who retain IP rights over their own work in compliance with DfE guidance.

Legal Disclosures

While interactions with the chatbot are anonymised, please be aware that Public Sector Analytics Ltd, our parent company, may be required to disclose information in cases where there is a legal safeguarding duty to report, such as instances involving danger to oneself or to others.

General Information

Changes to Policy: We reserve the right to modify this policy at any time. Changes will be posted on our website, and continued use of our services will indicate your acceptance of these changes.

Contact Us: If you have any questions or concerns about this policy or the data we hold, please contact our Data Protection Officer at info@askkira.com.

By using our Services, you agree to the terms of this Privacy and Data Policy. Your privacy and the security of your data are of utmost importance to us.

The most current version of this policy will always be available on our website.

Last updated: 5 January 2026