Public Sector Analytics Limited

DATA PROTECTION IMPACT ASSESSMENT

Company No 14889377 · askkira.ai

V1.0/Autumn Term 2025

Audience: UK School Staff Only (Teachers, Leaders – Not Pupils)

Date Completed: [Insert Date]

Completed by: [Insert Name / Role]

Reviewed by DPO: [Insert Name / Date]

This DPIA outlines how Public Sector Analytics Limited handles personal data in UK schools. askKira is a secure AI- powered platform providing teacher tools, including marking support, lesson planning, communication, wellbeing support and professional dialogue. It processes user-generated queries and interaction logs. The aim is to ensure data is handled lawfully, fairly, and transparently while reducing risk to individuals' rights.

1. Scope and Description of Processing

Data Subjects: Teachers, senior leaders, support staff (18+, professional use only).

Data Types: Staff names, school emails, job roles, school name, usage metadata (login time, frequency), conversation transcripts.

No pupil data is required or encouraged.

Data entered only by authorised adult users with professional school emails.

Used in UK schools and MATs for professional purposes only.

2. Purpose and Lawful Basis

Purpose: Reduce staff workload, enhance teaching efficiency, support wellbeing, and provide AI-generated assistance for school-related queries.

Lawful Basis:

• Contract (Article 6(1)(b)) – to deliver the service to subscribed institutions.

• Legitimate Interests (Article 6(1)(f)) – for anonymised analytics and insights (where opted-in).

Special category data is not intentionally collected.

The platform does not use data for marketing or profiling.

3. Nature of Processing

AI-generated support for lesson planning, marking, SEND strategies, and wellbeing tools.

All data processed securely, with session logs for functionality and safeguarding.

Schools/MATs remain Data Controllers. askKira acts as Data Processor.

4. Consultation

Input from education professionals, DPO, and technical staff.

School pilot feedback included in development.

Sub-processors reviewed and under contract.

Users agree to terms at sign-up and can access privacy details.

5. Risk Assessment and Mitigation

Risks Identified:

Unauthorised access.

Misuse of AI-generated content.

Entry of sensitive data.

Mitigations:

Secure login, UK-hosted infrastructure.

Staff training materials provided.

Reminders not to enter sensitive/pupil-identifiable data.

Session logging with deletion policies.

Data deleted within 30 days of contract termination; backups purged within 90 days.

Low to medium residual risk under current controls.

6. Data Protection Principles

Lawfulness, Fairness, Transparency: Clear explanations and accessible privacy policy.

Purpose Limitation: Data used solely to support teaching/workload.

Data Minimisation: Only essential staff data collected.

Accuracy: Users review inputs and outputs.

Storage Limitation: Data retained only as required (see retention policy).

Integrity & Confidentiality: Encryption, role-based access, secure sub-processors.

7. Rights of Individuals

Access: Staff can request their data.

Correction: Users can amend inputs.

Deletion: Staff may request erasure (“right to be forgotten”).

Restriction: Users can choose what data to input.

Portability & Objection: Supported on request.

8. International Transfers

Primary hosting in UK (AWS London).

In rare cases, processing may occur in the EEA/USA under UK–US Data Bridge and SCCs.

9. Subprocessors

askKira uses the following sub-processors, all bound by UK GDPR:

Infrastructure: AWS (UK – London), Microsoft Azure.

AI: OpenAI (API, no training on customer data), Google Gemini.

Education Data Access: Wonde (MIS integration).

Security/Performance: Cloudflare (DDoS protection).

Analytics: Google Analytics (EEA), Hotjar (anonymised).

Communications: Google Workspace, Mailchimp.

Payments: Stripe (PCI-DSS compliant).

Finance: Xero (accounting).

10. Outcome

Data processing is proportionate, supporting staff workload and wellbeing.

Risks are low/medium with mitigations in place.

Aligned with DfE AI guidance (2025) and Ofsted AI findings (2024/25).

11. Ongoing Monitoring and Review

DPIA reviewed annually or after significant changes.

DPO to monitor updates and manage queries.

Staff encouraged to raise concerns/feedback.

12. Additional Safeguards

Platform does not directly interact with children.

Schools retain controller role and oversee use.

All data entry must comply with school safeguarding/data policies.

askKira provides DPIA templates and support for schools to meet statutory requirements.

Records of Processing Activities (Article 30) maintained by askKira.

13. Cyber Security Standards

Cyber Essentials certified.

Regular penetration testing.

Follows ISO 27001 principles for information security.

Staff trained in data security.

14. Insurance and Liability

askKira maintains insurance cover to protect clients:

Public Liability: £2,000,000

Professional Indemnity & Products Liability: £2,000,000

Employers' Liability: £10,000,000

15. Contact

Data Protection Lead Contact: [Name of staff member]

Name: [School/MAT DPO]

Email: [DPO Contact Email]

Phone: [Optional]

16. Version Control

DPIA Version: v1.1 (Autumn 2025)

Date Completed: [Insert Date]

Next Review Due: [Insert Date]

Reviewed by: [Name/Role]