askKira.com

ACCESS AND AUDIT NOTE (TEMPLATE)

AUTUMN TERM, 2025

Template for UK Schools and Multi-Academy Trusts. This note explains who can use our AI tools, how they get access, what we record, how we check it's safe, and what to do if something goes wrong.

Organisation: <*School/MAT name*>
Owner:
Authors/Reviewers: <*IT Lead/DPO/DSL*>
Approved by: <*Head/CEO/Governors*>
Version: v1.0
Effective date:
Next review due: <*Term/Date or "on statutory update"*>

Who can use our AI tools

- Staff may use only the approved tools listed here: <*link/location*>.
- For staff tasks only (planning, drafting, resources).
- Do not paste personal or sensitive information about pupils, parents or staff unless you have written permission and it's covered by our DPIA.
- Follow our Acceptable Use Policy (AUP) at all times.

Getting access

- Ask your Line Manager. You'll get access after a 10-minute briefing and signing the AUP.
- Sign in with your school/MAT login (Single Sign On). No personal accounts.

Changing roles or leaving

- If your role changes, we adjust your access.
- When you leave, we remove access the same day and transfer any work files to your team.

What we record (logs)
We keep basic records so we can keep everyone safe and meet our legal duties.

- We log who used a tool, when, which tool/feature, and how long prompts/outputs were (approx.).
- We do not log your content by default.
- If we must see content for short-term troubleshooting, we'll limit it to admin/test accounts, keep it no longer than 72 hours, and protect it. This only happens with DPO approval.

askKira.com

DRAFT AI STRATEGY STATEMENT

AUTUMN TERM, 2025

Where logs are kept and who can see them

- Logs are stored in <*system/location*>.
- Only IT, the AI Lead, and the DPO can access them.

How we check (audit)

- **Monthly:** quick check for unusual use (e.g., very high volumes or late-night spikes).
- **Half-termly:** the DPO checks we're not collecting unnecessary data; the DSL reviews any safeguarding flags.
- **Termly:** a short report goes to SLT and governors (usage, impact, incidents, fixes).

Red flags we look for

- Use of unapproved tools.
- Repeated attempts to paste personal/sensitive data.
- Unusual volumes or access from unusual locations.
- AI use during assessment windows where it isn't allowed.

What to do if something goes wrong

- Report immediately via <*helpdesk/email/phone*>. Examples: accidental data pasted, suspicious output, deepfake/misinformation, or access you don't recognise.
- We triage within 24 hours (*AI Lead + IT + DPO; DSL if safeguarding*).
- If needed, we follow our breach procedure and ICO timelines and let affected people know.

Vendors and data

- We only use vendors with a Data Processing Agreement and clear data location and deletion terms.
- Where possible, data stays in the UK/EU. On exit, we confirm deletion.

Where key records live

- Approved Tools List: <system/location>
- AI Register (Article 30): <system/location>
- DPIAs: <system/location>
- Incident/Breach Log: <system/location>
- Audit evidence:<system/location>

askKira.com

DRAFT AI STRATEGY STATEMENT

AUTUMN TERM, 2025

Who to contact

- **AI Lead:** <*name/email*>
- **IT Helpdesk:** <*name/email*>
- **DPO (Data Protection):** <*name/email*>
- **DSL (Safeguarding):** <*name/email*>

Review schedule

- This note is reviewed termly for checks/audits and annually (or sooner if DfE/Ofsted/ICO/JCQ guidance changes).

SIMPLE ACCESS LEVELS (EXAMPLE)

ROLE	WHAT YOU CAN DO
All Staff	Use approved tools for drafting and resources (no personal data).
Champions	As above plus help colleagues and share safe prompts.
AI Lead	See usage summaries and manage settings.
IT Admin	Manage logins and integrations (no content view by default).
DPO	See audit exports and DPIA links (metadata only).
DSL	See safeguarding-related alerts if needed.
Vendor Support	Short-term, limited access for fixes; logged and removed when done.