

KEEPING IT SAFE: WHAT TEACHERS NEED TO KNOW ABOUT AI AND DATA

AUTUMN, 2025

AI tools can make a big difference to teaching - saving time and supporting pupils in new ways. But before using platforms like askKira, ChatGPT, Claude or Gemini, it's important to understand your responsibilities around GDPR and safeguarding. If pupil data is involved, making sure you're compliant isn't just a nice-to-have - it's a must. All data input must follow your school's safeguarding and data entry guidelines, especially when using new or external tools.

1. Typing in pupil names

If you write:

"Write a report for Ellie-Mae in Year 4 about her behaviour this term..."

You've just shared personal data.

✗ Names = personal data = GDPR breach.

2. Sharing sensitive information

If you say:

"James has an EHCP and attachment issues - give me a strategy to support him..."

That includes special category data - which is protected by law.

✗ Medical needs, SEND, safeguarding, and family issues should never go into AI.

3. Pasting real pupil work

Uploading writing from a pupil or copying a message from a parent, even without a name, can still identify someone - especially in small schools.

✗ Even "just for marking help" = a breach if it's not anonymised.

4. Using AI to write emails about pupils

Asking it to write:

"An email to Ruby's mum about her poor attendance"

includes identifiable data and private issues.

✗ You wouldn't post it online - so don't type it into AI.

KEEPING IT SAFE: WHAT TEACHERS NEED TO KNOW ABOUT AI AND DATA

AUTUMN, 2025

5. Assuming AI is private

It isn't! Think of it like this:

Anything you write in AI could be read by someone else later.

6. Forgetting school systems

If you're using AI instead of your school's systems (like Arbor, CPOMS, MyConcern), you might be putting data in the wrong place.

✗ Important pupil info should stay inside your school's secure systems.

Quick Rule to Remember:

"Would I say this out loud in a busy café or post it on Twitter?" If the answer is no, don't put it into AI.

Top Tips to Stay Safe and GDPR-Compliant

1. All data input must follow school safeguarding and data entry guidelines.

✗ Don't include:

- Pupil names
- Initials
- Birthdays
- Medical info
- EHCP details
- SEN status
- Behaviour logs
- Home circumstances

✓ Do say instead:

"A Year 5 pupil with dyslexia needs help understanding a text on rivers."

Rather than: "Can you simplify this for Ruby in Year 5, who has dyslexia and a reading age of 6?"

KEEPING IT SAFE: WHAT TEACHERS NEED TO KNOW ABOUT AI AND DATA

AUTUMN, 2025

2. Stick to anonymised prompts

Use placeholder terms like:

- "a pupil" instead of a name
- "Year 6" instead of class codes
- "SEND need" or "lower reading ability" instead of specific diagnoses

3. Check the tool's privacy policy

Not all AI tools are created equal. Free versions of tools may store data and use it for training. If your school hasn't provided a safe list of tools, ask your DPO (Data Protection Officer) or DSL (Designated Safeguarding Lead).

4. Use school-approved platforms

Some AI tools are designed for school use and come with GDPR compliance built-in. If your MAT or school has a contract with one, use that instead of public-facing tools.

5. Avoid using AI for sensitive topics

Safeguarding flags like disclosures, behavioural concerns, family issues, or bullying should never be discussed via AI tools. These must go through your normal safeguarding reporting system (CPOMS, MyConcern, etc).

6. Log use as part of your teaching process

If you're using AI to support planning or resource creation, consider noting it in your planning documentation. Transparency is key, especially if Ofsted or parents ask where certain materials came from.

7. Ask if you're unsure

Not sure whether something is okay to input? Treat it like safeguarding: **If in doubt, leave it out** - and ask. Speak to your DSL, DPO, or tech lead.