

Choosing an AI App - Safety Checklist (for everyday users)

You don't need to understand how AI works to use this checklist. It's designed to help you spot common warning signs and make safer choices. If you're not confident in using AI, [our free online courses](#) will give you everything you need to do so well and to stay safe.

In this checklist, an app means any digital tool you use on your phone, computer, or through a website. This includes things you download, websites you type into, and AI chat tools you talk to. This guide helps you decide whether a specific AI tool is likely to be safe to use but it's not a guarantee that something is safe. Only use apps your organisation has approved for use.

1. Who made it?

Stay Safe	Red Flags
A named company or organisation with a real website and contact details. Ideally, a reputable provider such as Microsoft, Google, Open AI or Anthropic	No company name, no website, or only a generic email address.
Clear information about who is responsible for the app.	You cannot tell who runs it or where they are based.

2. What data does it collect?

Stay Safe	Red Flags
A clear, plain-English privacy policy.	Vague wording about data use.
Explains how your data is used and where it is stored.	No privacy policy at all.

3. Can you delete your data?

Stay Safe	Red Flags
A clear option to delete your data or account.	No deletion option.
Explains how long deletion takes.	Tells you to email support instead.

4. Does it ask for unnecessary permissions?

Stay Safe	Red Flags
It only asks for access (permissions) to data it needs.	Requests access that does not make sense.
The app still works if you deny extra permissions.	Access to contacts, microphone or location without reason.

5. Is the AI behaviour appropriate?

Stay Safe	Red Flags
States clearly that it is an AI, not a human.	Claims to be a friend, partner or therapist.
Avoids sexualized, or manipulative behaviour.	Gives medical, legal or financial advice.

6. Does it have safety features?

Stay Safe	Red Flags
Reporting tools and content filters.	No way to report problems.
Age-appropriate safeguards where relevant.	Markets itself as uncensored or without limits.

7. Is it clear how they make money?

Stay Safe	Red Flags
Clear pricing and subscription information.	Hidden subscriptions.
No surprise charges.	Sudden paywalls after sign-up.

8. Does it integrate with reputable platforms?

Stay Safe	Red Flags
Available via official app stores or known platforms.	Only downloadable from unknown websites.
Uses trusted technology providers.	Suspicious or fake reviews.

9. Does it avoid harmful claims?

Stay Safe	Red Flags
Honest about its limits.	Claims guaranteed results.
Uses calm, factual language.	Calls itself an AI doctor or therapist.

10. Does it feel safe overall?

Stay Safe	Red Flags
Feels transparent and respectful.	Pushy behaviour.
Nothing feels rushed or pushy.	Anything that feels off or uncomfortable.

Quick 10-Second Test

Avoid the app if two or more of these apply: its not clear who the company is, it has no readily available privacy policy, asks for unnecessary permissions, or makes extreme or inappropriate claims.

How to check if a specific app is likely to be safe

Here's a prompt you can amend and paste into your AI (such as Copilot) to check if it is likely to be safe, or not.

*Help me check whether this AI app is safe to use. Here's the **name of the app and what it does**. Please assess it using a safety checklist: who made it, data use, permissions, behaviour, safety features, business model, and any red flags. Also check app-store reviews, user complaints, and any media coverage to see if people have raised concerns about scams, safety issues, privacy problems, or inappropriate behaviour. Use official links, such as developer website, privacy policy, terms, security page, and the official App Store/Google Play listing and evidence-based citations: "If you can't find/verify a link, say so — don't guess.". Split links into: Primary sources (official) vs Independent sources (reputable reporting / consumer bodies).*

If you wish to, you could then follow this by asking it about a specific context that may affect risk, such as:

- The intended **user group**: adult, young person/child, an ethnic or faith community.
- **Safeguarding** considerations: vulnerable users, power imbalance, dependency risk.
- **Personal safety** considerations: harassment, stalking, coercive behaviour risks or.
- **Data sensitivity** concerns: personal identity, location, images.

However, AI cannot give you a definitive “safe/unsafe” verdict. It can only assess risk indicators based on available information and it can make mistakes. Treat this as a screening checklist, then confirm by checking the official developer pages and independent sources before entering any personal, confidential, or payment information.

Using AI Meeting note takers

The guidance above applies to AI meeting note takers but we also have a [free ‘bite size’ 20min online course](#). This provides much more specific guidance on choosing and using these and includes downloads and a policy that you can amend and use in your organisation.

How this checklist was created

This checklist was created using AI and is based on real-world patterns seen in AI apps. It draws on issues identified by consumer protection bodies, app-store investigations, data-protection regulators, and documented user complaints. It highlights the behaviours most commonly found in unsafe apps and the safety practices consistently used by reputable providers.



Help us to help everyone by sharing this with your network. [Charity Excellence Learning](#): certificated, online AI courses that anyone can undertake.