

What never goes in the prompt

Rules for using AI at work



What never goes in the prompt: rules for using AI at work

Which information may go into which AI tool, what counts as checked before anyone relies on the output, and what the courts and regulators have already written down. Each rule is traced to the public document behind it, or marked as this brief's own.

Written for team leads, practice managers, HR leads and whoever owns data protection in an organisation of 10 to 250 people, writing or checking the rules for staff use of AI tools.

What goes in, and where it goes

A rule about AI at work is tested in the seconds before someone pastes. The Department for Science, Innovation and Technology's UK Business Data Survey, run from October 2025 to January 2026, found that 17 per cent of small businesses using AI (10 to 49 employees) and 22 per cent of medium ones (50 to 249) had a formal, written policy. The answers are self-reported and weighted, from 1,870 AI-using businesses of all sizes.

The common assumption is that a paid account makes a tool safe for client material. The Solicitors Regulation Authority warned solicitors on 17 August 2026 that free and paid AI systems alike may pose risks to client confidentiality: depending on the provider's terms, settings and technical architecture, what is entered may be stored, retained or used to improve the tool. Guidance to judges says anything put into a public AI chatbot "should be seen as being published to all the world". The classes and rules below are this brief's; the last column gives their grounds.

Class	What it covers	The rule	Basis
Red	Special-category data, such as health records; legally privileged advice; OFFICIAL-SENSITIVE material	Never into a public tool or a personal account; only into a system approved for that class	UK GDPR Article 9(1); SRA notice, on privilege; Security Classifications
Amber	Other personal data; client-confidential documents	Approved tools only, on business accounts whose terms bar training on the data and limit retention	SRA notice
Green	Material already published or cleared for publication	Any approved tool; the output is still checked	Judicial guidance; AI Playbook
Unclassified	Anything nobody has placed yet	Treated as red until its owner decides	None: a default

An AI app may request permissions that reach other information on the device; the judicial guidance says to refuse them all and to use work devices. Before an AI tool is deployed, the AI Playbook says to review access controls so that users reach only data they may view.

What checked means

The common assumption is that checking a citation means confirming the case exists. In *AI-Haroun v Qatar National Bank*, decided with *Ayinde v Haringey* by the High Court on 6 June 2025, many of the cited cases that did exist did not contain the quotations attributed to them or support the propositions cited. The SRA now asks that every case cited to a court be genuine, relevant, verifiably cited and advancing the argument.

42

reports related to the potential misuse of AI reached the SRA between July 2025 and July 2026. Reports, not findings: the SRA says a number of investigations are ongoing.

Solicitors Regulation Authority, 17 August 2026

18 of 45

citations in *AI-Haroun* were to cases that do not exist. The claimant said they came from publicly available AI tools, legal search engines and online sources.

High Court, [2025] EWHC 1383 (Admin), paragraphs 74 and 76

The court said that freely available generative AI tools are not capable of reliable legal research, and that anyone using AI for it has a professional duty to check it against authoritative sources before using it in their professional work (paragraphs 6 and 7). The routines below are this brief's; the last column gives the duty or risk behind each.

Output	Checked means	Basis
A citation or quotation	Found in an authoritative source, with the quoted words present and the point supported	Ayinde, paragraphs 6, 7 and 74; SRA notice
A figure	Traced to the publisher's own table, with its date, base and caveat	Judicial guidance: output may be inaccurate, incomplete or out of date
A summary	Compared with the underlying document by someone who has read it	Judicial guidance: care is needed to ensure a summary is accurate
A draft letter	Names, dates, amounts and commitments checked against the file by the sender	SRA notice: whoever uses AI remains accountable for the work

The obligations already written down

The Information Commissioner's Office says in its AI guidance that in the vast majority of cases the use of AI will involve processing likely to result in a high risk to people's rights and freedoms, which legally requires a data protection impact assessment. That guidance is under review after the Data (Use and Access) Act 2025. On 30 September 2026 the Commissioner's functions pass to a new Information Commission.

The common assumption is that Article 22 of the UK GDPR still governs automated decisions, as the ICO's own page on it still said when this brief was checked. Articles 22A to 22D replaced it, in force for all purposes since 5 February 2026. A significant decision based solely on automated processing, meaning with no meaningful human involvement, now needs safeguards that let the person be informed of it, make representations, obtain human intervention and contest it.

The Care Quality Commission lists eleven principles that providers using AI to deliver health and social care in England must follow, including human oversight, training, and systems to recognise, report and investigate when something goes wrong.

Whoever decides whether a slip is a breach has to be named before the first slip. Pasting personal data into an unapproved tool can be an unauthorised disclosure, part of the UK GDPR's definition of a personal data breach. A breach must be notified to the regulator without undue delay and, where feasible, within 72 hours of becoming aware of it, unless it is unlikely to result in a risk to people's rights and freedoms; every breach must be documented.

Sources

Department for Science, Innovation and Technology, UK Business Data Survey 2026, Official Statistics, published 18 June 2026. Section 3.4 on AI governance (figure 18 and the breakdown by size), the introduction on fieldwork and weighting, and the size labels.

Solicitors Regulation Authority, 'SRA cautions profession about safe and responsible use of AI in legal sector', news release, 17 August 2026.

Solicitors Regulation Authority, 'Misuse of AI', warning notice, published 17 August 2026. Sections 'AI hallucinations: relevant considerations' and 'Client confidentiality: relevant considerations'.

High Court (Divisional Court, King's Bench Division), R (Ayinde) v London Borough of Haringey and Al-Haroun v Qatar National Bank QPSC [2025] EWHC 1383 (Admin), judgment of 6 June 2025, paragraphs 6, 7, 74 and 76.

Courts and Tribunals Judiciary, Artificial Intelligence (AI): Guidance for Judicial Office Holders, 31 October 2025. Section 3, parts II, III and V, and section 4.

UK GDPR, Article 9(1), processing of special categories of personal data, as revised on legislation.gov.uk.

UK GDPR, Article 22A, automated processing and significant decisions, inserted by the Data (Use and Access) Act 2025, section 80, with the textual amendment note.

UK GDPR, Article 22C, safeguards for automated decision-making, paragraphs 1 and 2.

UK GDPR, Article 4(12), definition of a personal data breach.

UK GDPR, Article 33(1) and (5), notification and documentation of a personal data breach.

Information Commissioner's Office, Guidance on AI and data protection, chapter 'What are the accountability and governance implications of AI?', section 'Why are DPIAs required under the data protection law?', and the page's review notice.

Information Commissioner's Office, 'Rights related to automated decision making including profiling', UK GDPR guidance page, as retrieved 19 September 2026.

The Data (Use and Access) Act 2025 (Commencement No. 9 and Transitional and Saving Provisions) Regulations 2026, SI 2026/1015, regulation 2; made 10 September 2026.

Care Quality Commission, 'Artificial intelligence in health and social care: CQC's role, expectations and plans', page last updated 21 May 2026. Section 'What does this mean for providers?'.

Cabinet Office, Government Security Classifications Policy (HTML version), updated 5 August 2024, paragraph 25 on the -SENSITIVE marking.

Government Digital Service, Artificial Intelligence Playbook for the UK Government, published 10 February 2025. Sections on public AI applications, embedded applications and plugins, security risks, and practical recommendations.

What this brief is not

It is not legal advice and not a compliance checklist: following it does not make an organisation compliant with the UK GDPR, the EU AI Act or any regulator's rules, and it certifies nothing. It names no AI product and compares none. It describes public documents as they stood on 19 September 2026, several of which changed during 2026 and may change again. We teach and build with AI tools, and readers should weigh the brief accordingly.

Theo Coleman

Chief Technology Officer, BespokeWorks. September 2026