15 clauses to complete

AI acceptable use policy

[Organisation], version [number], [date]

Each clause is short on purpose: a rule staff cannot recite is one they will not follow.

1. **Purpose and scope** This policy governs the use of artificial intelligence tools in the course of work for [Organisation]. It applies to all employees, contractors, temporary staff, volunteers and directors, on any device including their own, and whether or not [Organisation] provided the tool. It covers tools reached through a browser, an application, a plugin, an extension, a feature embedded in another product, or an API. Where it conflicts with a client engagement term or a professional obligation, the stricter requirement applies.

2. **Definitions** AI tool means any system that generates, summarises, classifies, transcribes or predicts using a model, including features embedded in products you already use. Input means anything a user types, pastes, uploads, dictates or connects to one. Output means what it returns. Client information means any information relating to a client's affairs, whether or not the client provided it. Personal information has the meaning given by the privacy law applying to [Organisation].

3. **Approved tools, and how a tool gets approved** Only tools on the approved list in Annex B may be used for work, and only with input that clause 5 allows. The list names the tool, the plan or tier, the account type and the approver. A tool is added only after a named person has checked, in writing: what the vendor does with input, whether input trains models and whether that can be switched off, where data is stored, how long it is kept, and whether the contract is with [Organisation] rather than an individual. Free and personal tiers are not approved.

4. **What must never go into an AI tool** The data types listed in Annex A must never be entered into any AI tool, approved or not, in any form, including inside a screenshot, a pasted table, an uploaded file or a connected mailbox. This prohibition has no approval path. If a task seems to require it, stop and escalate to the person named in clause 15.

5. **What may go in, and on what condition** Input not listed in Annex A may be entered into an approved tool once it has been cut to the minimum the task needs and direct identifiers removed or replaced. Removing a name is not removing an identity: a matter number, a rare job title, or a date plus a location can identify a person on its own. Replacing an identifier with a code does not take the information outside privacy law for [Organisation], which holds the mapping. Keep the mapping between codes and real values outside the AI tool.

6. **Client confidentiality is a separate duty** Confidentiality obligations apply to AI tools as to any other third party. Entering client information into a tool run by another organisation is a disclosure to a third party. Where an engagement letter, retainer, professional rule or contract requires client permission before such a disclosure, that permission is obtained before the information is entered, and recorded.

7. **Personal information and privacy law** Personal information may be entered into an approved tool only where that is consistent with the purpose it was collected for and permitted by the privacy law applying to [Organisation]. [Organisation] remains responsible for it after it enters a tool, including for its security. Where the regulator recommends against a category of input,

that recommendation is followed unless a named person records a reason not to.

8. **Consent, engagement letters and notices** Where clause 6 requires client permission, it is obtained in the engagement letter, a signed consent or an equivalent written record, and states what will be disclosed, to whom, where the data will be stored, and that AI tools may be used. Privacy notices and the privacy policy describe the use of AI tools in terms an individual can understand.

9. **Human review before reliance** Output is a draft. No output may be sent to a client, filed, published, relied on in advice, or used to decide something about a person until a competent human has checked it against a source. The reviewer is accountable for the content as if they had written it. Citations, figures, quotations, legislative references and calculations are checked one by one against the primary source, never against another AI tool.

10. **Disclosure and marking of AI assisted work** Where content generated or materially altered by an AI tool is published, given to a client, or filed with a court, tribunal or regulator, [Organisation] discloses that fact where a rule, contract or professional obligation requires it, and wherever a reader would otherwise be misled. Staff do not remove or defeat any marking or metadata a tool attaches to its output.

11. **Records: the use case register** [Organisation] maintains the register in Annex D. Each approved use case records the tool, the purpose, the categories of input, who approved it, the date, and the next review. Prompts and outputs on client matters are kept in the matter file under normal record keeping rules, not only inside the tool's own history.

12. **Accounts, plans and vendor terms** Work input is entered only through accounts held in [Organisation]'s name, on the plan named in the approved list. Personal accounts, personal email addresses and consumer tiers are not used for work input. Where a tool offers a setting controlling whether input trains models, or how long it is retained, the setting is recorded in the approved list and checked at each review.

13. **Devices, browsers and extensions** Browser extensions, plugins, desktop assistants and integrations that can read a page, a document or a mailbox are installed only from the approved list. Staff do not connect an AI tool to a mailbox, a document store, a practice management system or a code repository without approval under clause 3.

14. **Incidents** If prohibited data has been entered into an AI tool, or anything into an unapproved one, the user reports it to the person named in clause 15 the same day. Nobody is disciplined for reporting promptly. [Organisation] records what was entered, when, into which tool and under which account; asks the vendor to delete it and records the answer; and assesses whether the incident is notifiable. Under Australia's Notifiable Data Breaches scheme, the test includes whether a reasonable person would conclude it would be likely to result in serious harm.

15. **Owner, review cycle and changes** This policy is owned by [named role]. It is reviewed at least every twelve months, and whenever a tool is added to the approved list, a regulator publishes guidance that changes a clause, or an incident under clause 14 exposes a gap. Every version carries a date and a change log. Staff are notified of material changes and acknowledge again using Annex C.

ANNEX A: DATA THAT MUST NEVER BE ENTERED

Category	Australia	Spain	Caught by a local detector?

Government identity number	Tax file number (TFN)	DNI, NIE	Yes, check digit; the TFN only after its label
Health identifier	Medicare number, Individual Healthcare Identifier	Número de la Seguridad Social	Yes, check digit; Medicare and Seguridad Social numbers only after their label
Business number tied to a person	ABN of a sole trader	NIF de autónomo	Yes, check digit; the ABN only after its label
Bank and card details	BSB and account number, card number	IBAN, card number	Card number yes, check digit and a known issuer. IBAN yes, check digit. BSB and account number only after the words "BSB", "Bank State Branch" or "account number". See how
Client names and matter details	Any	Any	Partly: names in a labelled field, a signature or after a title such as Mr or Dr, by position rather than by a list of ours. Matter numbers after the words "matter number", and never the matter itself
Property identifiers	Title reference, full address	Referencia catastral, full address	Address yes, by position; title reference no. The cadastral reference, only after its label, is masked visibly, never replaced without telling you: its check algorithm is unofficial and fails in the four foral territories and can fail on rural parcels
Health information	Diagnoses, records, results	Health data (Article 9 GDPR)	Partly: record numbers after their label, never the diagnosis or result itself
Criminal history	Charges, convictions, police records	Criminal records	Partly: case numbers after their label, never the charge or conviction itself
Biometric data	Face, voice, fingerprint templates	Biometric data	No
Credentials	Passwords, API keys, tokens	Passwords, API keys, tokens	Some API keys and tokens yes, passwords no. Do not rely on a detector here

ANNEX B: THE ONE PAGE SHEET

Yes, with an approved tool	No, never
Rewriting your own draft with no client details	Anything in Annex A
Summarising a public document	Client names and matter details
Drafting a template letter with no client details	Uploading a client file
Generating test data	Pasting a whole document to "check" it
Explaining a concept you then verify	Anything you would not email to a stranger
Code with no credentials or client data in it	Credentials, keys and tokens

ANNEX D: USE CASE REGISTER

Use case	Tool and plan	Input categories	Approved by	Date	Next review

ANNEX C: ACKNOWLEDGEMENT

I have read the [Organisation] AI acceptable use policy dated [date].

Name: _____ Signature: _____ Date: _____