Ready • Ai • Go

THE PRACTICAL WORKBOOK

Company AI guidelines template

Clear rules. Confident employees. Responsible AI at work.

A practical structure for defining how your team may, or may not, use AI.

Practical AI.
Human judgment.

20 sections to shape your company guidelines

BEFORE YOU BEGIN / A PRACTICAL STARTING POINT

Make these guidelines your own

The best AI guidelines reflect how your business actually works.

Choose what matters to your business

Every organisation uses AI differently. Some sections in this workbook will be directly relevant to your team; others may have little bearing on your day-to-day work. You do not need to adopt every suggested rule or complete every section.

Use the guidance selectively. Start with the topics that matter most to your business, the information you handle and the ways your employees use AI. Adapt the wording, choose the options that fit and add examples from your own workplace. Leave out sections that do not apply, while checking that your final guidelines cover your responsibilities and risks.

Aim for clear, usable guidance
A focused set of rules that employees understand and can apply is more useful than a long document that is difficult to follow. Review your draft with the relevant people in your organisation before sharing it.

Help employees understand the rules

Clear rules work best when people understand the reasons behind them. Ready AI Go offers a range of practical training to help employees build confidence with AI and recognise its limitations and risks.

Topics include everyday AI use, prompting, privacy, checking AI-generated information and recognising AI-enabled threats. Use training alongside your company guidelines to help employees put the rules into practice.

Share and maintain your guidance digitally

Once you have agreed your guidelines, you can enter them into Ready AI Go and make them available digitally to everyone in your company. This gives employees a shared place to find the rules that apply to their work.

Keeping your guidance in Ready AI Go makes it easier to share and maintain as your tools, working practices and business needs change. Review it regularly so your team can refer to clear, up-to-date guidance.

Choose what applies. Make it clear. Help your team put it into practice.

01–02 / PURPOSE & SCOPE

Set the direction

A practical structure for defining how employees may — and may not — use AI at work.

How to use this workbook
Adapt the rules to your organisation, data, tools and risk profile. Complete the fields and select the options that apply. This is a working template, not a finished policy. Have legal, privacy, security and compliance stakeholders review it before publication.

01 Purpose of these guidelines

Explain why you are introducing AI guidelines. Help employees use AI responsibly, with clear boundaries and human judgement.

Our organisation allows employees to use AI to:

Examples: brainstorm ideas, draft documents, summarise, improve writing, translate non-sensitive content, analyse approved datasets, assist with code, research and automate repetitive work.

Suggested principle
Employees may use AI when it does not expose confidential information, create unacceptable risk, violate company policies or replace required human judgement.

02 Who these guidelines apply to

These guidelines apply to:

- ☐ All employees
- ☐ Contractors
- ☐ Freelancers
- ☐ Interns
- ☐ External partners
- ☐ Specific departments only

They apply when AI is used:

- ☐ On company devices
- ☐ On personal devices for work
- ☐ Through company accounts
- ☐ Through personal AI accounts for work
- ☐ In customer-facing work
- ☐ For internal work

Other people, departments or situations:

03 / APPROVED TOOLS

Choose your AI tools

Give employees an explicit list of approved tools, uses and restrictions.

Be specific. “Use trusted AI tools” leaves too much room for interpretation.

03 Which AI tools employees may use

Tool / account	Approved use	Restrictions

Possible restrictions: company-managed accounts only; enterprise environment only; no free/public version; no third-party integrations; non-confidential information only; approved departments only.

Tools requiring approval

Responsible person / team:

Tools and conditions requiring approval:

Prohibited tools

These AI tools may not be used for company work:

Define the boundary
Employees may not introduce a new AI tool into company workflows without approval from the person or team named below.

Approval owner:

04 / INFORMATION & AI

Define your data boundaries

Employees should not have to make complex privacy and security decisions every time they open an AI tool.

04 What information may be entered

GREEN / Approved information

Information employees may enter into approved AI systems. Examples: public information, published website content, product descriptions, marketing material, generic questions, fictional examples and specifically approved non-sensitive internal information.

Our GREEN information includes:

AMBER / Restricted information

Use only in specifically approved tools or under defined conditions. Examples: internal documents, processes, meeting notes, business performance, source code, research and anonymised customer-related information.

Our AMBER information includes:

AMBER: approved tools and required conditions:

RED / Never enter into public or unapproved AI

Examples: passwords, API keys, credentials, confidential customer or personal data, medical or financial account information, employee records, contracts, trade secrets, strategy, proprietary datasets, security architecture, non-public financial information and sensitive intellectual property.

Our RED information includes:

RED information must never be entered unless both the system and the specific use case have been explicitly approved.

RED exceptions may only be approved by:

05–06 / PRIVACY & CONFIDENTIALITY

Protect people and company data

Set clear rules for information about employees, customers, prospects, partners and your organisation.

05 Personal and customer information

Personal data may:

- ☐ Never be entered into AI systems
- ☐ Only enter specifically approved systems
- ☐ Be used when properly anonymised
- ☐ Be used in approved circumstances

Other conditions / approved circumstances:

Personal information employees must never enter:

When uncertain whether information is personal or sensitive, do not upload it. Ask the person or team named below first.

Privacy contact:

06 Confidential company information

Copying information into an AI chat can mean sharing it with another system or provider. Define what your organisation considers confidential.

Employees may not enter these into unapproved AI systems:

- ☐ Internal financial information
- ☐ Strategy or board documents
- ☐ Contracts
- ☐ Customer information
- ☐ Employee information
- ☐ Intellectual property
- ☐ Product roadmaps
- ☐ Internal emails
- ☐ Source code
- ☐ Security information
- ☐ Credentials or access keys
- ☐ Unpublished research

Other confidential information / company-specific examples:

07–08 / REVIEW & HUMAN JUDGEMENT

Keep people accountable

AI may assist employees. Employees remain responsible for the work they produce and the decisions they make.

07 AI-generated information must be checked

AI-generated information must not automatically be treated as factual. Verify important information before relying on it.

Check facts, statistics, quotes, sources, references, customer information and business recommendations. Take particular care with legal, financial, medical, technical and security information.

Before AI-generated work is used externally, employees must:

- ☐ Review it themselves
- ☐ Verify important factual claims
- ☐ Check referenced sources
- ☐ Have another employee review it
- ☐ Obtain manager approval
- ☐ Follow existing quality controls

Additional verification requirements:

08 Human responsibility

AI must not independently make final decisions about:

- ☐ Hiring or firing
- ☐ Employee evaluation
- ☐ Promotions or compensation
- ☐ Customer eligibility
- ☐ Credit or financial decisions
- ☐ Legal decisions
- ☐ Safety-critical decisions
- ☐ Medical decisions
- ☐ Security incidents
- ☐ Other: _____

For these activities, AI may:

- ☐ Not be used at all
- ☐ Only assist with preparation
- ☐ Suggest; a person must decide
- ☐ Follow a separate approved procedure

Additional rules / required human decision-maker:

09–10 / CUSTOMER CONTENT & MEDIA

Set standards for external content

Define what employees can create, publish or send to customers, and which checks are required first.

09 Customer-facing AI content

AI-generated customer-facing content:

- ☐ Is allowed after human review
- ☐ Requires manager approval
- ☐ Is limited to specific content types
- ☐ May not be used

Allowed content types / other conditions:

AI-generated content may not be used for:

Before publishing or sending externally, employees must:

10 AI-generated images, audio and video

Employees may use generative AI for:

- ☐ Marketing images
- ☐ Internal presentations
- ☐ Concept development
- ☐ Audio
- ☐ Video
- ☐ Voice generation

Employees may not:

- ☐ Impersonate real people
- ☐ Create misleading content or fake customer testimonials
- ☐ Present generated media as evidence of an event that did not happen
- ☐ Use another person's likeness without appropriate permission

Other permitted uses / additional media rules:

11–12 / COPYRIGHT & SOFTWARE

Protect intellectual property

Apply the same care to AI-assisted creative work and code as you would to other company work.

11 Copyright and intellectual property

Do not assume AI-generated material is automatically safe for commercial use. Before using it, consider:

- ☐ Has third-party material been reproduced?
- ☐ Do logos, trademarks or copyrighted characters appear?
- ☐ Is confidential company intellectual property being shared?
- ☐ Do licensing conditions apply?
- ☐ Can the output be used legally for its intended purpose?

Our rules for AI-generated intellectual property:

12 AI for software development

Approved coding assistants / environments:

Developers may not submit:

- ☐ Production credentials
- ☐ API keys
- ☐ Customer data
- ☐ Proprietary source code
- ☐ Security-sensitive code
- ☐ Internal architecture information

AI-generated code must:

- ☐ Be reviewed by a developer
- ☐ Pass existing testing procedures
- ☐ Pass security checks
- ☐ Be checked for licensing concerns
- ☐ Follow normal code review
- ☐ Other: _____

Additional restrictions or development rules:

13–14 / FRAUD & PROHIBITED USES

Recognise threats. Set firm limits.

AI can make scams more convincing. Give employees a clear verification procedure and clear boundaries.

13 AI-generated scams and suspicious content

Verify unusual requests involving money transfers, payment details, bank changes, password resets, credentials or confidential files. Take care with unexpected executive or customer requests, including convincing voices and images.

If an employee receives a suspicious request:

1.

2.

3.

Report suspected AI-enabled fraud to:

14 Things employees must never use AI for

- ☐ Upload prohibited company information
- ☐ Upload customer information without approval
- ☐ Circumvent security controls
- ☐ Generate malicious software
- ☐ Create fraudulent or deceptive content
- ☐ Impersonate another employee or customer
- ☐ Make unauthorised automated decisions
- ☐ Send AI-generated output without required review
- ☐ Use unapproved AI tools for company work
- ☐ Present AI-generated research as verified fact without checking it

Other prohibited uses specific to our company:

1.

2.

3.

15–16 / QUESTIONS & INCIDENTS

Make it easy to ask and report

A useful policy gives employees a clear next step when the answer is uncertain or something goes wrong.

15 What employees should do when unsure

If you are unsure whether information can be entered into an AI system, do not enter it until you have checked.

Questions: name / team and email / channel:

Ask for approval before using a new tool, entering sensitive data, automating an important decision, connecting AI to another company system or introducing a new customer-facing AI process. Ask whenever a use case may not comply.

16 Reporting mistakes and incidents

Report accidental uploads of confidential or customer information, exposed credentials, suspected AI-enabled fraud, harmful or misleading output used externally, and unapproved AI connections.

If an incident occurs, immediately contact:

Include in the report	Details
AI tool used	
Information shared	
Date and time	
People potentially affected	
Action already taken	

Encourage fast reporting
Mistakes can happen. Employees should report accidental misuse promptly and should not attempt to hide it.

17–19 / TRAINING & GOVERNANCE

Turn guidelines into a habit

Assign an owner, teach the rules and set a regular review cycle.

17 Training requirements

All employees must complete:

- ☐ AI fundamentals
- ☐ Prompting
- ☐ AI-generated scam awareness
- ☐ Role-specific AI training
- ☐ AI privacy
- ☐ AI security awareness
- ☐ AI hallucination awareness
- ☐ Other: _____

Training must be completed:

- ☐ When joining the organisation
- ☐ Annually
- ☐ When major AI policies change
- ☐ Before using AI tools
- ☐ Through ongoing short training
- ☐ Other: _____

18 Who owns AI governance?

AI policy owner — name / department:

The owner is responsible for:

- ☐ Maintaining the approved-tool list
- ☐ Reviewing new AI use cases
- ☐ Coordinating employee training
- ☐ Updating these guidelines
- ☐ Handling AI incidents
- ☐ Monitoring AI developments

Other responsibilities:

19 Review your guidelines regularly

Review the guidelines:

- ☐ Every 3 months
- ☐ Annually
- ☐ When requirements or legislation change
- ☐ Every 6 months
- ☐ When a major AI system is introduced
- ☐ Following an AI-related incident

Last reviewed: _____ **Next review:** _____

Review owner:

20 / EMPLOYEE QUICK REFERENCE

Your AI guidelines at a glance

Complete this page after agreeing your policy. Share it with employees as a practical, two-minute reference.

Organisation: _____ **Version / date:** _____

We allow employees to use AI for:
_____

01 Which tools can I use?

You may use:

02 What information can I put into AI?

You may enter:

03 What information must never go into AI?

Never enter:

04 What must I check?

Always verify / required reviewer:

05 What do I do when I am unsure?

Ask — name / team and contact details:

Unsure? Pause and ask before you upload.

FINAL CHECK / FROM POLICY TO BEHAVIOUR

Ready to put it into practice?

Before publishing, make sure your guidelines answer the questions that matter.

- ☐ Do employees know which AI tools are permitted?
- ☐ Do employees know which AI tools are prohibited?
- ☐ Have we defined what information must never enter AI?
- ☐ Have we defined rules for personal and customer data?
- ☐ Do employees understand that AI can be incorrect?
- ☐ Do we require human review for important decisions?
- ☐ Have we set rules for external and customer-facing output?
- ☐ Do employees know how to report an AI-related mistake?
- ☐ Does someone own and maintain these guidelines?
- ☐ Have employees been trained on the rules?
- ☐ Have we set a date to review the guidelines again?

If several answers are “no”, a policy alone is probably not enough. Employees need to understand why the rules exist and how to apply them in real situations.

From AI policy to AI behaviour

Writing guidelines is the first step. Helping employees understand and follow them is the next.

Ready AI Go turns AI rules into practical employee knowledge through short, ongoing training in AI use, prompting, privacy, hallucinations, AI-generated threats and responsible behaviour.

Set up your company.
Add your employees.
Assign their training.

Free for companies with up to 15 employees.