

PRACTICAL AI / BEFORE YOU SHARE INFORMATION

AI Data Handling Pre-Flight Guide

Use this check before you paste, upload, dictate or connect business information to an AI tool.

Choose the least information and the most controlled tool that can complete the task. If the information is not suitable for a public website, check before using it in an unapproved AI tool.

01 The 60-second check

- 1. What work am I trying to complete, and what information is truly needed?
- 2. Who owns the information, and who could be affected by its use?
- 3. Is it public, internal, confidential, personal or sensitive?
- 4. Is this provider, product and business account approved for this exact use?
- 5. What could happen if the information or output is wrong, exposed or misused?
- 6. Can I use a smaller extract or synthetic example instead?

Task or workflow

Person responsible

What information is truly needed, and why?

Fill the shaded fields in a PDF reader that supports forms, or print and write. Save a copy, close it and reopen it to check your entries. Keep answers brief; use a separate sheet for more detail. Do not enter passwords or other secrets.

General operational guidance, not legal advice. Obligations depend on the business, people affected, information, provider, contracts and applicable law. Pause and obtain qualified advice where authority or coverage is uncertain.

AI DATA HANDLING / INITIAL DECISION

Choose the handling path

Make this decision before the information leaves the business. A handling path records the next check; it is not a score.

Use the highest applicable information class. If you are unsure, take the more protective path and ask the person responsible for privacy, security or operations.

Proceed with care	The input is public and appropriate to reuse, or genuinely generic or synthetic. The business account is approved, no credentials or unnecessary personal details are included, and a person will check the output.
Pause and check	Internal, confidential or personal information is needed; the tool is new or consumer-facing; a contract or client instruction may apply; the output will be sent externally; or the provider's data use, access or retention is unclear.
Stop and escalate	Credentials, sensitive or restricted information, a suspected breach, security vulnerability, complaint, dispute or unclear authority require designated review. Take extra care with information about children or vulnerable people and decisions affecting employment, credit, insurance, eligibility, safety or legal rights.

Do not put passwords, API keys, recovery codes or authentication tokens into prompts or uploads. Do not automate a consequential decision from an unchecked AI output.

These paths are internal operating controls, not a statement that every listed use is prohibited by law. Approval must address the actual purpose, information, tool and safeguards.

Initial handling path

☐ Proceed with care ☐ Pause and check ☐ Stop and escalate

Reason and the authority or safeguard that needs review

Person who must review

Review date or evidence reference

AI DATA HANDLING / CLASSIFICATION AND MINIMISATION

Keep only what the task needs

One file may contain several information classes. Remove what the task does not need before the AI service receives it.

Public	Published web copy or opening hours. Check currency, rights and unnecessary personal details.
Internal	Process notes or draft plans. Use a short authorised extract in an approved account.
Confidential	Pricing, contracts or supplier terms. Check authority and terms; use a generic example where possible.
Personal	Names, contact details or customer history. Check the privacy process and purpose; minimise identifying detail.
Sensitive or restricted	Health, biometric, identity or security information. Pause by default; obtain designated review and safeguards.

Removing a name may not be enough

A person may still be identifiable from other details or when records are combined. Assess re-identification risk in the actual sharing environment. Use synthetic examples for initial tests when you cannot establish a safe approach.

- ☐ Replace names with roles or placeholders where useful.
- ☐ Use a range, total or category instead of a raw record.
- ☐ Use a short factual extract rather than an entire document.
- ☐ Exclude credentials and unnecessary payment or identity details.

Information needed and highest applicable class

What will we keep, remove or replace?

Fictional example, not client evidence

The full project update contains client names and commercial notes. The owner excludes it and approves a synthetic topic list for the initial agenda test. Removing names alone would not establish that the original file is safe.

OAIC: De-identification and the Privacy Act

AI DATA HANDLING / PROVIDER AND ACCOUNT

Check the exact tool and account

Approval must cover this task, product tier, account, settings, integrations and the people who can access the information.

- ☐ This provider, product tier and business account are approved for the task.
- ☐ Access, retention, training use, deletion, security and incident terms have been reviewed.
- ☐ Only people who need access can use the account, integration or shared output.
- ☐ Data location, overseas access, subprocessors and contractual restrictions have been considered.
- ☐ Someone can pause, disable or fall back from the AI-assisted process.
- ☐ The output receives human verification proportionate to its possible impact.

Provider, product tier and business account

Settings or terms evidence reference and date checked

Purpose and information class

Minimisation decision

Accountable owner

Reviewer and date

Conditions of use

Next review date or change trigger

Unknown settings, ownership, authority or safeguards are reasons to pause. Do not treat a checked box or a paid account as proof that every future use is acceptable.

AI DATA HANDLING / LOW-RISK TESTS

Test the handling and review path

Use synthetic or other approved low-risk test material first. Check output before sending, publishing or using it for a consequential action.

Normal: result and evidence

Accuracy, completeness and source

Correction or next action

Incomplete: result and evidence

Missing information and uncertainty are flagged

Correction or next action

Ambiguous: result and evidence

No unsupported assumption is presented as fact

Correction or next action

Exception: result and evidence

The workflow pauses, escalates and falls back safely

Correction or next action

Fictional example, not client evidence

The synthetic topic list gives no date. The draft adds one. The reviewer removes it, records the failed incomplete-information test, revises the instruction and retests.

No customer message, publication, purchase, contract, regulated action, material claim or consequential decision should proceed solely from an AI output.

Person reviewing the test outputs

What remains unresolved before approval?

AI DATA HANDLING / DECISION AND CONDITIONS

Record permission for this use

The decision covers only the purpose, information, account and safeguards recorded here. Revisit it when those conditions change.

Choose one decision

- ☐ Approved with conditions ☐ Revise and retest ☐ Do not proceed

Owner and reviewer

Decision date and next review trigger

Purpose, permitted information and approved account

Conditions, exclusions and required human review

Decision reason and supporting evidence reference

Fictional example, not client evidence

Approved with conditions for synthetic agenda-topic tests only, in the approved business account with manual review. The original project update stays excluded. Fix the invented-date failure before using the result. Real internal records require a fresh information review.

This example approves the stated test scope only. It is not permission to use the original file or release an unchecked output.

Continue with the AI Workflow Starter Checklist

OAIC: privacy and commercially available AI products

National AI Centre: Guidance for AI Adoption

ASD ACSC: Engaging with artificial intelligence

Source references carried forward from the 2 October 2026 edition. General operational guidance, not a legal determination or compliance certification.