Where Client Data Is Allowed to Go

An approved AI account still leaves your team with a question: can this information go into it for this job? Write down which tools people may use and what data is allowed there. If either is unclear, ask for approval before pasting, uploading or sharing it.

I made this companion to the one-page AI policy template so you can fill in those decisions. Your team shouldn't have to interpret a provider's privacy agreement while finishing a client report, that is work the firm needs to do first.

Name the tool, account and work it is approved for

For the owner: Start with the actual account people will use, not just the product name. Fill in a row for each approved tool and account, adding rows when different uses have different limits.

Tool and account	Approved work	Allowed data	Restrictions	Checked by / date
[Tool and account]	[Work allowed]	[Data types]	[Limits on use]	[Name / date]

Check the agreement and settings for training on submitted data, how long data is kept, who can access or share it, and what happens when other services are connected.

Those checks matter, but they don't override a client's restrictions. Check the client's terms and any legal or professional requirements before approving the use, including whether consent is needed.

Write down what can and cannot go in

Now make the data limits specific. “Protect confidential information” still leaves someone deciding what confidential means while looking at a spreadsheet. Give them a list they can use.

Data type	Allowed or prohibited	Conditions / approved tool
[Type of information]	[Allowed or prohibited]	[Where it may go and any limits]

For example, take comparing software for managing customer relationships, often called CRM software. The row below shows how you could fill in the sheet, it isn't a record of an approved account at my companies.

Data type	Allowed or prohibited	Conditions / approved tool
Public product descriptions for a software comparison	Allowed after the firm approves the use	[Approved tool and account]. Exclude personal information and confidential client records.

How we draw the line at my companies

At my companies, we check the tool provider's privacy agreement first. Our internal tools have no training on data and no data retention, and our policy still prohibits confidential data in them.

Data	Rule at my companies
Market information, competitor information and public information	Allowed within our privacy rules, with the exclusions below.
Personally identifiable information (PII), meaning information that identifies a person	Prohibited.
Financial data with a company name or other details that identify the company	Prohibited.
Other confidential data	Prohibited, even in approved internal tools.

Information being public doesn't cancel those exclusions. And removing a company name doesn't give permission to upload financial data that still identifies it through other details.

These are the rules at my companies, not a claim that our list answers every firm's obligations. Use them as an example while you write your own.

Ask before using anything outside the rules

If the list doesn't cover the work, people need someone to ask. Fill in the contact and a response time your firm can support.

Request owner: [Name]

Request channel: [Where to ask]

Expected response time: [Time]

For the team: Check the completed tool and data lists before use. If they don't cover the work, explain in your request what the job is, how it works today, which tool or change you need and what type of data is involved.

Describe the data without attaching anything prohibited.

At my companies, people bring these requests to a forum. Operations first looks at the process and where AI should come into it, then we evaluate the software with the tech team and decide whether to buy, build or update an existing tool before deploying the change.

Usually, the user can have a response in a few days. That is a response, not a promise that the change will be deployed by then.

While waiting, they cannot use the unapproved tool or move the work to another unapproved account. There is no point in having a policy if people are just going to go over the policy and put the work somewhere else, right?

Check it before the team uses it

This is an operator's starting template, not legal advice or a claim that it meets every obligation. Have your legal adviser check it against your jurisdiction, industry, contracts and actual tools before adopting it.

Policy owner: [Name]

Effective date: [Date]

Next review: [Date]

Current policy and tools-list location: [Link or location]

Report suspected data exposure to the policy owner promptly.

Once the fields are filled and the review is done, put the sheet where people can reach it.

Then walk through the software-comparison example with the team: public product descriptions in the approved account, a client contact list that contains prohibited personal information, and a request to use a tool that hasn't been approved. Ask someone to show you what they would do in each case.