



Handling data safely

What counts as data, what goes into AI tools, how to keep it safe day to day, and what to do when something slips.

Ekalavya Academy by Almost Magic

Short Book 4 of 10 | Free to read and share

almostmagic.net.au

BEFORE YOU START

How to read this book

1

Learn

A few slides explain one idea in full sentences.

2

See it

A short, made-up example gives the idea a face.

3

Try it

A ten-minute exercise in the tools you already use.

4

Check it

Three questions. Guidance is at the back, not next to the question.

5

Keep it

A four-sentence summary to come back to.

Two levels in every chapter. The main slides are written so a first-time reader can follow them. A "Going deeper" slide gives the same idea at the level an experienced reader would argue about.

This book works with any AI tool you already have. It never asks you to buy or sign up for a particular product.

THE PLAN

Where this book sits in the series

Book 1	What AI is, and what it is not	Foundations
Book 2	Productivity with AI: writing, summaries, research, meetings	Practical use
Book 3	From one task to a repeatable workflow, and AI deputies	Workflow automation, agents
Book 4	Handling data safely	Data handling
Book 5	When a data shortcut becomes the rule	Data quality and governance
Book 6	Staying secure with AI	Security
Book 7	Rules, risk and what you must know	Risk and compliance awareness
Book 8	Your AI rules on one page	Policy and accountability
Book 9	When AI gets it wrong	Recovering from AI mistakes
Book 10	When not to use AI, and who stays in charge	Judgement and oversight

Each book works on its own. Read them in order or pick the one you need.

CONTENTS

In this book

Chapter 1

What counts as data

Chapter 2

What goes into AI tools

Chapter 3

Keeping data safe day to day

Chapter 4

When something goes wrong

At the back

Guidance and answers for every question and exercise

CHAPTER 1

What counts as data

By the end of this chapter you will be able to:

Name the main kinds of data in a small business.

Tell personal information from other data.

Find where your data lives.

Label data as public, internal or sensitive.

Time: about 40 minutes, including the exercise.

LEARN

Data is more than a spreadsheet

Data is any record about people, money, work or things: customer lists, invoices, emails, photos, staff files, quotes, passwords and notes on a client.

Much of it lives in places you do not think of as data, such as inboxes, chat threads, shared drives and phones.

Before you can protect it, you need to know what you have and where it is.

IN PLAIN WORDS

If it is written down, it is data.

LEARN

Common kinds in a small business

Customer details

Names, addresses, phone numbers, orders and complaints.

Staff records

Pay, leave, performance, health and contact details.

Money

Invoices, bank details, prices, margins and payroll.

Contracts and plans

Agreements, quotes, tenders and strategy.

Access details

Passwords, codes, keys and account logins.

Public material

Website text, brochures and published prices.

LEARN

Three levels

A simple three-level label is enough to start. Add more only if you need them.

Public

Anyone may see it. A tool can usually use it freely.

Internal

For your team only. Not harmful if it slips out by accident, but not for outsiders.

Sensitive

Harmful if it leaks: personal details, money, health, passwords and confidential deals.

GOING DEEPER

Personal information and context

Personal information

Information about an identifiable person. Many places have privacy laws about collecting, using and sharing it. Check the rules that apply to you.

Combining data

Two harmless facts can identify someone when put together, such as a job title and a small town.

Hidden details

Files and photos can carry hidden details, such as author names, locations and edit history.

Data held for others

Data that belongs to a customer or supplier is held on trust. Your permission to use it may be narrower than you think.

SEE IT

A short example

Rosa runs a small physiotherapy clinic. She lists what data the clinic holds: patient notes, appointment times, invoices, staff rosters and website text.

She is surprised to find that appointment reminders on a staff phone, and a shared inbox, also hold patient names.

She labels notes and names as sensitive, the roster as internal and the website as public.

THE LESSON

List first. Protect second.

This is a made-up example for teaching.

TRY IT

Map your data

1

List ten kinds of data your business holds.

2

Mark where each one lives: inbox, drive, phone, paper or other.

3

Label each one public, internal or sensitive.

4

Circle the three you would least want to leak.

YOUR TOOLS

Use any notes app or paper. Do not paste real customer data into a tool for this exercise.

GUIDANCE

What to look for is on slide 44.

CHECK IT

Check yourself

Question 1

Name the three levels in the simple label.

Question 2

Why can two harmless facts together be a problem?

Question 3

Whose permission matters when you use a customer's data in a new way?

Answer in your own words before you turn to slide 44.

KEEP IT

Chapter 1 in four sentences

KEEP THIS

Data is any record about people, money, work or things, and much of it sits in inboxes, chats and phones. Label it public, internal or sensitive. Personal information has its own rules, and data held for others is held on trust. List first, then protect.

CHAPTER 2

What goes into AI tools

By the end of this chapter you will be able to:

Decide what may be pasted into an AI tool.

Understand where data goes after you press send.

Find the settings and terms that matter.

Use stand-ins instead of real details.

Time: about 40 minutes, including the exercise.

LEARN

Where your data goes

When you paste text or upload a file, it is sent to the company that runs the tool. What happens next depends on the tool, the plan you use and your settings.

Some tools may keep what you send, let staff review it or use it to improve their systems. Others offer settings or business plans that limit this. The only way to know is to read the terms and settings for the tool you use.

A tool on your own computer or in your own building keeps data closer to home, but still needs care.

REMEMBER

Pressing send is sharing.

LEARN

Sort before you paste

A rule of thumb to apply to each item before you paste it.

Safe

Public material, and made-up or generic examples.

Ask first

Internal documents and anything about a named customer or staff member. Check the tool's terms and your organisation's rules.

Never

Passwords, payment card numbers, health records, and anything you are not allowed to share.

LEARN

Use stand-ins

Replace names

Use Customer A and Supplier B instead of real names.

Round and generalise

Use a range or a rounded figure when the exact one does not matter.

Cut what is not needed

Paste the paragraph you need, not the whole file.

Keep the key to yourself

Keep your own list of who Customer A is. Do not give it to the tool.

LEARN

Questions to ask about any tool

Does it keep my data?

Look for how long, and whether you can delete it.

Does it learn from my data?

Look for settings or plans that turn this off.

Who can see it?

Staff of the tool's company, other users, or only you.

Where is it stored?

Some rules limit sending personal information overseas. Check what applies to you.

GOING DEEPER

Redaction is harder than it looks

Hidden identifiers

An unusual job, a rare product or a date can still point to one person even when the name is gone.

Files carry more

A document can hold comments, tracked changes and metadata that you cannot see on the page.

Screenshots

A screenshot can show names, tabs and notifications in the background.

Plan differences

Free, personal and business plans of the same tool can have different data terms. Check the plan you actually use.

SEE IT

A short example

Kofi manages a small recruitment agency. He wants help tidying a candidate summary and is about to paste in a CV.

Instead he replaces the name and contact details with "Candidate A", removes the previous employers' names and pastes only the skills section. He keeps a note of who Candidate A is.

The tidy-up is just as useful, and he has shared much less.

THE LESSON

Share the least that still works.

This is a made-up example for teaching.

TRY IT

Plan a safe request

1

Take a real task where you would like AI help.

2

List the data it would need.

3

Sort each item: safe, ask first or never.

4

Rewrite the request with stand-ins and only what is needed.

YOUR TOOLS

You do not need to paste anything for this exercise. Plan the request on paper.

GUIDANCE

What to look for is on slide 45.

CHECK IT

Check yourself

Question 1

What happens to data when you paste it into an AI tool?

Question 2

Name two stand-in techniques.

Question 3

Why check the plan you use, not just the tool?

Answer in your own words before you turn to slide 45.

KEEP IT

Chapter 2 in four sentences

KEEP THIS

Pasting is sharing, and what happens next depends on the tool, the plan and your settings. Sort each item as safe, ask first or never. Use stand-ins, paste only what you need and keep the key yourself. Read the terms for the plan you actually use.

CHAPTER 3

Keeping data safe day to day

By the end of this chapter you will be able to:

Collect and keep less.

Control who can see what.

Store and delete AI outputs sensibly.

Use accounts and sharing settings safely.

Time: about 40 minutes, including the exercise.

LEARN

Collect less, keep less

The safest data is data you do not have. Collect only what you need, and delete it when you no longer need it.

This also applies to what you put into AI tools and what they give back. Chat histories and saved outputs can hold sensitive details.

Decide how long you keep things, and make deleting part of the routine.

RULE OF THUMB

If you do not need it, do not keep it.

LEARN

Who can see what

Least access

Give each person only the access they need for their job.

Separate accounts

Everyone uses their own login. Shared logins hide who did what.

Review regularly

Check who has access every few months and remove people who left or changed role.

Sharing links

Check whether "anyone with the link" is switched on. Prefer named people.

LEARN

Your AI outputs are data too

Chat history

Old chats may hold pasted details. Delete what you do not need, if the tool allows it.

Saved files

Drafts and summaries made from sensitive material are sensitive too. Store them with the originals.

Copies

Outputs pasted into emails or chats make more copies. Know where they went.

Shared accounts

If several people use one AI account, they may see one another's history.

LEARN

Accounts and devices

Use a strong, unique password for each account, and a password manager to keep track of them.

Turn on two-step sign-in where it is offered.

Keep devices and apps updated, and lock screens when you step away.

IN PLAIN WORDS

Good habits beat clever tricks.

GOING DEEPER

Why minimising beats protecting

A smaller target

Data you never collected cannot be stolen, leaked or misused.

Fewer obligations

Less personal information means fewer rules to follow and fewer people to tell if something goes wrong.

Easier checking

A short list of what you hold is easier to review than a sprawling one.

Backups and copies

Deleting also has to reach backups and copies. Know where those are.

SEE IT

A short example

Hui Min runs a small accounting firm. She finds that her team has saved summaries of client files in a shared AI chat history that all five staff can open.

She moves the summaries into the client folders with the right access, deletes the chat history and asks everyone to use their own accounts.

Two weeks later one team member leaves, and removing their access takes five minutes.

THE LESSON

Tidy as you go.

This is a made-up example for teaching.

TRY IT

Audit one tool

1

Open one AI tool you use and look at its history and sharing settings.

2

Note what sensitive details are stored there.

3

Delete or move what you do not need.

4

Write one habit you will keep, such as a weekly clean-up.

YOUR TOOLS

Use any tool you already have.
Only look at your own account.

GUIDANCE

What to look for is on slide 46.

CHECK IT

Check yourself

Question 1

Why does each person need their own login?

Question 2

Why are AI summaries of sensitive files themselves sensitive?

Question 3

What does least access mean?

Answer in your own words before you turn to slide 46.

KEEP IT

Chapter 3 in four sentences

KEEP THIS

Collect less and keep less. Give each person their own login and only the access they need. AI outputs and chat histories are data too, so store and delete them with care. Strong, unique passwords and two-step sign-in are basic habits that work.

CHAPTER 4

When something goes wrong

By the end of this chapter you will be able to:

Recognise a data slip early.

Know the first steps to take.

Know that you may have to tell others.

Learn from it without blame.

Time: about 40 minutes, including the exercise.

LEARN

Slips happen

Common slips: pasting something you should not have, sending a file to the wrong person, sharing a link that is open to everyone, or losing a device.

A fast, calm response matters more than perfection. Most harm comes from slips that were hidden or delayed.

Make it easy and safe for people to say "I made a mistake".

REMEMBER

Report early. Blame later,
or never.

LEARN

The first steps

1. Stop

Stop the spread. Remove the link, recall the message or close the session.

2. Tell

Tell the person who owns data rules in your business, straight away.

3. Note

Write down what happened, when, what data and who might be affected.

4. Fix

Change passwords, delete copies, ask recipients to delete, and ask the tool's company about deletion where possible.

LEARN

When you may have to tell others

In some places the law requires an organisation to notify affected people and a regulator about certain data breaches. In Australia, the Notifiable Data Breaches scheme applies to organisations covered by the Privacy Act, when a breach is likely to cause serious harm.

Not every small business is covered, and rules differ by country. Do not guess. Check the regulator's guidance or ask an adviser, and do it quickly.

Source: Office of the Australian Information Commissioner, "When to report a data breach" ([oaic.gov.au](https://www.oaic.gov.au)).

REMEMBER

Check the rules for where you operate.

GOING DEEPER

Learning without blame

Look at the system

Ask what made the slip easy, such as a confusing setting or a rushed deadline, before asking who did it.

Near misses count

Catching a mistake before harm is useful information. Record near misses too.

Small changes

Fix the cause with a small change: a default setting, a checklist item or a short rule.

Share the lesson

Tell the team what happened, with details removed, so others avoid it.

SEE IT

A short example

Ibrahim runs a small electrical business. He realises he pasted a customer address list into an AI chat to tidy it.

He closes the session, deletes the chat, checks the tool's settings and tells his office manager within the hour. They note what was shared and decide whether anyone needs to be told.

They also add a rule: customer lists are never pasted. Staff hear about it without his name attached.

THE LESSON

Act fast, write it down, fix the cause.

This is a made-up example for teaching.

TRY IT

Plan your response

1

Think of a data slip that could happen in your business with an AI tool.

2

Write the first four steps you would take.

3

Name who you would tell, and how to reach them.

4

Write one small change that would make the slip less likely.

YOUR TOOLS

Planning on paper is enough.

GUIDANCE

What to look for is on slide 47.

CHECK IT

Check yourself

Question 1

What are the first steps after a data slip?

Question 2

Why record near misses?

Question 3

Why should you not guess whether you must notify someone?

Answer in your own words before you turn to slide 47.

KEEP IT

Chapter 4 in four sentences

KEEP THIS

Slips happen, and a quick report matters more than a perfect record. Stop the spread, tell the right person, write down what happened and fix the cause. In some places you must tell affected people and a regulator, so check the rules and do not guess. Look at the system, not just the person.

AT THE BACK

Guidance and answers

Questions and exercises stay in the chapters, on their own slides.
Guidance lives here, so you can try first and look afterwards.

Try the task or question in your own words, then compare. Where your answer differs, that is worth a note, not a correction.

WHERE TO FIND IT

Slides 44 to 47: answers
and exercise guidance, one
slide for each chapter.

GUIDANCE

Chapter 1: answers and guidance

Answer 1

Public, internal and sensitive.

Answer 2

Together they can identify a person. A job title and a small town may point to one individual.

Answer 3

Check what the customer agreed to and the rules that apply. A new purpose may need fresh permission or may not be allowed. If unsure, ask before you do it.

Exercise

Most people find sensitive data in places they did not expect, such as phones and shared inboxes. Those are the places to protect first.

GUIDANCE

Chapter 2: answers and guidance

Answer 1

It is sent to the company that runs the tool. What happens next depends on the tool, plan and settings, so read the terms for yours.

Answer 2

Any two of: replace names, round figures, cut what is not needed, keep the key to yourself.

Answer 3

Free, personal and business plans of the same tool can have different terms for keeping and using your data.

Exercise

A strong answer names what was removed and what was kept. If the stand-in version would not still get you the help you need, the task may not suit AI.

GUIDANCE

Chapter 3: answers and guidance

Answer 1

Shared logins hide who did what, and make it hard to remove one person's access.

Answer 2

They hold the same details in shorter form, so they need the same care as the originals.

Answer 3

Each person gets only the access they need for their job.

Exercise

Most people find old chats holding details they forgot. If you found none, check saved files and shared folders too.

GUIDANCE

Chapter 4: answers and guidance

Answer 1

Stop the spread, tell the right person, write down what happened, and fix the cause and the copies.

Answer 2

They show weak points before harm happens, and give you a chance to fix the cause.

Answer 3

Rules differ by place and by organisation, and a wrong guess can add harm. Check the regulator's guidance or ask an adviser.

Exercise

A good plan names a real person and a real way to reach them. If you could not name one, that is the first thing to fix.

FIND OUT MORE

About Ekalavya Academy

Ekalavya Academy is a learning series from Almost Magic Tech Lab. The books are written for people who teach themselves, using the tools they already have.

Almost Magic builds tools that help people check and govern their AI use. The books never depend on those tools.

LINKS

Almost Magic: almostmagic.net.au

Case studies: ai-casestudies.almostmagic.net.au

Page for this book on the Academy site: link to be added when the page exists.