Keeping It Clean

Quick Reference

One-page summary of Playbook 3. Print, pin up, hand out.

1. Watch the contact, not the content

The information isn't dangerous. The context is.

2. Pause before data moves

Three questions, ten seconds. Same as checking the date on the milk.

3. Tell someone quickly

The worst version of any incident is the one nobody knew about until later.

Five places things tend to go wrong

1	**Paste into chatbot**	Customer data into a free AI to draft a reply. The information has left your systems.
2	**Personal account**	Forwarding to your own email or cloud because work is slow. Protections don't follow it.
3	**Unsanctioned workflow**	A useful tool you signed up for, connected to work systems. Data flow invisible.
4	**Shared document**	Folder shared last year. People have left. Settings unchanged. Contents have changed.
5	**AI output**	Summary or draft that contains confidential content that should not travel with it.

The pause: three questions

1. **What kind of information is this?** Personal, special category, commercial, internal, public.
2. **Where is it going to end up?** Sanctioned tool? Personal account? Outside the organisation?
3. **Would I be comfortable if my organisation could see this happening?** If no, that's information.

Categories worth recognising

Personal	Identifies a real person. Names, contacts, accounts.
Special category	Health, ethnicity, sexuality, politics, biometrics, religion.
Commercial	NDA-covered. Pricing, strategy, client lists.
Confidential	Personnel matters, internal plans, drafts.
Routine internal	Everyday operations. Not secret, not public.
Public	Marketing material, published reports.

Sanctioned vs not sanctioned

Sanctioned tools operate under contracts your organisation has signed. They don't train on your data by default. They log access. They sit within agreed boundaries.

Free or unsanctioned tools have none of that protection. The interface may look identical. The data posture is completely different.

A familiar logo isn't a guarantee. The same major vendors run both consumer and enterprise services side by side.

If something goes wrong

Tell someone quickly. The damage from a small incident reported early is almost always smaller than one hidden.

1. Tell your line manager.
2. Tell information governance or your DPO.
3. If sensitive data is involved, tell them today. The clock starts when someone reports it.

Reporting isn't a confession. It's a notification. The point is to limit consequences, not to apportion blame.

Who to ask

For…	Talk to…
Personal data questions	
Approved tools and access	
Reporting an incident	
"Is this allowed?" questions	
Training and learning	

Fill in the right contacts for your organisation.

RED LINES

Never put in consumer/free AI tools: personal data · special category data · commercially confidential · NDA-covered material · anything restricted.

Always get approval before: building or buying custom AI · AI making decisions about people · AI in service-user-facing services · personal data with AI at scale.