AI: Keep It Confidential.

Practical rules for using AI tools in day-to-day work without risking sensitive data.

cogio

Websites that get the point across.

Do

- **Remove personal identifiers before pasting:**
  Replace names, emails, phone numbers, addresses with placeholders like [Customer], [Telephone] etc.
- **Paraphrase sensitive text:**
  Summarise rather than sharing raw data or full documents.
- **Use company-approved accounts and settings:**
  Disable settings that allow your data to be used in training if available.
- **Keep an audit trail:**
  Save prompts, responses and outputs used in customer-facing messages in your own system. Don't rely on chat history for record-keeping.

Don't

- **Share sensitive information:**
  Passwords, API keys, card/bank details, medical data, or addresses.
- **Upload unredacted documents:**
  Customer lists, contracts, financial spreadsheets or invoices.
- **Share confidential information:**
  Pricing, intellectual property, security procedures or anything covered by NDAs.
- **Ask the model to make judgements for real cases.**
  Legal, financial or medical.
- **Use personal accounts or devices:**
  Company/customer information should remain on company assets.