



BDG TRAINING CONSULTANCY

PRACTITIONER GUIDE

The UK Investigator's AI Starter Pack

Ten structured prompts for investigative practice, each with the verification step and legal considerations it requires.

Written for investigators, enforcement officers and investigation managers in UK local authorities, the wider public sector and regulated industry.

Edition 1 · August 2026 · BDG Training Team

Before you start

Most investigators are already using AI. Comparatively few have been trained on it, and fewer still are working to a written policy that addresses investigative use. This pack is a starting point for doing it deliberately rather than by default.

A July 2026 survey of 500 UK professionals across banking, government and the public sector, legal, insurance and compliance, commissioned by compliance training provider Skillcast, reported that three quarters use AI at least weekly and more than three in ten use it several times a day. Sixty-nine per cent had received no formal AI training in the previous twelve months, and 48 per cent either had no workplace AI policy or did not know whether one existed — rising to 50 per cent in government and the public sector.

That gap is what this pack addresses. Not whether to use AI, but how to use it in a way that withstands scrutiny from a defence representative, an auditor, an information governance review or a court.

How each prompt is set out

ELEMENT	WHAT IT PROVIDES
What it's for	The specific investigative task the prompt supports.
Give it	What to supply for that prompt. See "Working from material you supply".
The prompt	Copy it, replace anything in square brackets, and supply your anonymised material.
The check	The verification step. This is not optional — it is what makes the output usable.
Watch-out	The legal or professional risk attaching to that particular task.

The prompts are written to work in any general-purpose assistant — Microsoft 365 Copilot, ChatGPT or Claude. Where the platform materially changes the risk position, this is noted.

Three principles that apply throughout

- ONE — AI ASSISTS, THE INVESTIGATOR DECIDES**

Every prompt here supports a task for which you already hold responsibility. None of them make a decision. If a prompt appears to be producing your professional judgement for you, it is being used incorrectly.
- TWO — UNVERIFIED OUTPUT CANNOT BE RELIED UPON**

Large language models produce fluent, confident and plausible text that is sometimes simply wrong: misstated statutory provisions, invented case citations, subtly altered facts. They can also carry bias, from their training data or from the material you supply. Fluency is not accuracy, and a neutral tone is not neutrality. Every output requires reference back to the source.
- THREE — RECORD THAT IT WAS USED**

Note in your decision log or case file where AI assisted, what it produced and how you verified it. This takes a single line, and it is the difference between a defensible process and a difficult conversation eighteen months later.

The policies you are working under

Three questions need settling before any prompt in this pack goes near case material. The first two are answered by your own organisation. The third depends on the powers you are working under.

Nothing here displaces your own organisation's policy. Where the two differ, your policy governs. This pack is written to be consistent with:

The AI Playbook for the UK Government. Ten principles for public sector AI use, including knowing what the technology can and cannot do, using it lawfully and responsibly, keeping meaningful human control at the right stages, and using the right tool for the job — which sometimes means not using AI at all.

Police use of artificial intelligence (Home Office factsheet), where policing is involved: lawful, ethical and transparent use, robust assessment before deployment, and decision-making authority remaining with the officer. The Equality Act 2010 and the Data Protection Act 2018 apply to AI use as they do to anything else.

IPCO's Scope of Interest in AI (26 March 2025), where RIPA or Investigatory Powers Act powers are engaged. This is dealt with as the third check overleaf.

- 1 What does your organisation's AI policy actually permit?** Many UK public authorities now have Microsoft 365 Copilot available within their Microsoft 365 environment. Corporate approval to deploy a tool is not the same as approval to use it on investigative material. Establish what your policy says about AI use in investigations specifically, whether you are required to record that AI assisted a piece of work, and who signs that off. If the policy is silent on investigations, that is worth raising rather than working around.
- 2 What security classification are your tools approved to handle?** Establish the highest Government Security Classification your AI tools are accredited for, and do not exceed it. The Government Security Classifications Policy (current version August 2024) sets three tiers — OFFICIAL, SECRET and TOP SECRET — with -SENSITIVE applied as an additional marking within OFFICIAL rather than as a separate tier. Investigation material held by local authorities and regulators will typically sit at OFFICIAL, often carrying the -SENSITIVE marking. Your information security or information governance team can tell you what your tenant is approved for. If you cannot establish it, do not put case material into the tool.

Investigatory powers and IPCO

- 3 **Are investigatory powers engaged?** Where AI is used in connection with the investigatory powers, it falls within the scope of interest of the Investigatory Powers Commissioner's Office. IPCO's scope covers AI used to make or enhance an application for a power, to assist or undertake authorised conduct, to analyse what that conduct obtains, and to review, retain, share or destroy it. Three points from IPCO's *Scope of Interest in AI* matter in everyday practice:

Commodity software counts. IPCO expressly includes AI features embedded in commonly used software, naming Microsoft 365. Copilot in your tenant is not outside this simply because it is not a specialist tool.

The label does not decide it; the effect does. Software its developers do not call AI still falls in scope if its effect is, or is expected to be, to significantly change the breadth or depth of intrusion into privacy.

The scope is covert activity. Overt investigatory techniques sit outside IPCO's scope of interest.

IPCO's central question is whether AI increases the number of subjects who can be investigated, and whether it changes the intended or collateral intrusion. That is a proportionality question, and it is yours to answer.

WHATEVER THE PLATFORM, NEVER ENTER THE FOLLOWING

- Names, addresses, dates of birth, National Insurance numbers or contact details of suspects, witnesses, victims or complainants
- Any material generated under a RIPA authorisation, and anything at all relating to a CHIS
- Unredacted witness statements, MG forms or case papers
- Case or reference numbers capable of identifying an individual or an operation
- Special category data and criminal offence data relating to identifiable people
- Anything covered by legal professional privilege
- Anything above the classification your tool is approved to handle

Anonymise as a matter of routine

Replace names with role labels — Witness A, Subject 1, Officer B. Replace addresses with “the premises”. Use relative dates where the exact date is immaterial. Every prompt in this pack is written to work on anonymised material, so this costs you nothing.

ONE POINT WORTH KNOWING ABOUT COPILOT

Where Copilot is deployed in your tenant, your prompts and its responses are captured in the unified audit log, fall within your authority's retention policies and are discoverable through eDiscovery — subject to those controls being switched on. That gives you a genuine audit trail. It also means what you typed about a live case is a record held by your organisation. Write your prompts as though a third party may read them.

Six things AI must never do

These hold regardless of platform, licence or local policy. They are not data protection points; they go to the integrity of the investigation itself.

- 1 Write your necessity and proportionality reasoning.** A RIPA rationale must be the authorising officer's own reasoning applied to these facts. Generated text is not reasoning, and would not withstand scrutiny by an inspectorate or a court.
- 2 Decide what is disclosable.** Under s.7A of the Criminal Procedure and Investigations Act 1996 and the Attorney General's Guidelines on Disclosure 2024, the prosecutor's duty of disclosure is a continuing one, subject to review until the conclusion of proceedings; the disclosure officer must also give a personal declaration that the task has been completed. Neither is capable of delegation to a tool.
- 3 Author a witness statement.** A statement must be the witness's own words, signed as true. AI-smoothed prose assists the cross-examiner and places the witness in an impossible position in the box.
- 4 Monitor or profile an individual.** Systematic use of AI tooling to build a picture of a person may amount to directed surveillance. The Covert Surveillance and Property Interference Code of Practice directs authorities to consider an authorisation where work involves repeated viewing of a subject or building up an intelligence picture. Local authorities must also meet the serious crime threshold and obtain magistrates' approval under s.32A RIPA. The tool will not alert you to any of this.
- 5 Serve as the source of a fact.** Nothing an AI tool asserts is evidence of anything. It indicates where material may be; the material is the evidence.
- 6 Replace your rationale in a decision log.** The log records why you decided what you decided. That is its entire function.

A NOTE ON THE WIDER REGULATORY DIRECTION

The Information Commissioner's Office consulted during 2026 on draft guidance covering automated decision-making and profiling. Separately, regulations made in April 2026 under s.124A of the Data Protection Act 2018 require the Commissioner to prepare a statutory code of practice on artificial intelligence and automated decision-making; no publication date has been set. The consistent theme across both is **meaningful human involvement** — a reviewer who genuinely can and does override the output, rather than one approving a recommendation in seconds. Investigation teams sit within scope, and the six points above anticipate that direction rather than merely reflecting today's position.

A NOTE ON SCOPE

Part I of the Criminal Procedure and Investigations Act 1996 applies to any person acting as prosecutor, and s.26 requires investigators who are not police officers to have regard to the CPIA Code. Local authority and regulatory investigators are therefore within the disclosure regime, and the Attorney General's Guidelines on Disclosure 2024 apply. Several of the prompts that follow refer to **Annex A** to those Guidelines, which deals with digital material, and to the **Investigation Management Document (IMD)**. The IMD is the investigator's document: it is where Annex A expects the digital strategy to be recorded. It then feeds the lawyers' **Disclosure Management Document (DMD)**, which is the prosecutor's document and the one through which the approach is explained to the court and the defence. Investigator writes the IMD; prosecutor writes the DMD; the IMD is not served on the defence.

Working from material you supply

You decide what goes in front of the tool. That judgement — what is proportionate, what is anonymised, what your policy and security classification permit — is yours, and it is not delegable. What follows is the instruction set that keeps the tool inside the boundary once you have decided.

What the tool is for, and what it is not

IT DOES THIS

Read, summarise, signpost

It reads material at volume, summarises it accurately against the issues you specify, and draws your attention to what may matter — including lines of enquiry pointing both towards and away from the suspect.

It may infer, provided it says so. An inference clearly labelled as an inference is useful; the same inference presented as a fact is not.

IT DOES NOT DO THIS

Apply the test

Whether material meets the relevancy test, whether it is sensitive or non-sensitive, and whether it satisfies the disclosure test — that it might undermine the prosecution case or assist the case for the accused — are decisions for the investigator and the disclosure officer.

The tool flags a fact for you to consider against the test. It does not reach the conclusion.

Preparing what you supply

Give it material in a form it can actually read — text rather than screenshots, with page or paragraph numbering intact so it can cite what it tells you, and anonymised as a matter of routine. Beyond that, keep it simple: the pointers under each prompt say what that prompt needs.

ONE LIMITATION WORTH KNOWING

A language model cannot read EXIF or file metadata from an image. Asked when a photograph was taken, it will produce an answer inferred from the content of the picture — the light, the season, the clothing — and may present it with more confidence than it deserves. Extract metadata with a proper tool and supply it as text, and tell the model to record it as not provided where you have not.

The grounding rules

Append these to any prompt where you supply material. They are what keeps the output tied to your documents rather than to the model's general sense of how cases like this tend to go.

GROUNDING RULES — apply to everything you produce from the material I supply:

1. Work only from the material provided. Do not draw on outside knowledge, or on general knowledge of similar cases.
2. Cite the source for everything — the document, and the page or paragraph.
3. Label clearly what the material STATES and what you have INFERRED from it. Inference is useful; inference presented as fact is not.
4. Where the material is silent or ambiguous, say so rather than completing it.
5. Where documents conflict, record both versions and identify each. Do not choose between them.
6. Do not apply any legal test. Where something may engage one, flag it for me to consider and explain why it may matter.
7. Do not characterise any person's intent, credibility or guilt.
8. Do not read metadata from an image. Where I have not supplied metadata as text, record it as not provided.
9. List at the end anything referred to in the material but not supplied to you, and anything you could not read or interpret.
10. Tell me where in this output you are least confident, and why.

Keep this to hand — it is worth more than any individual prompt in this pack. The ten prompts follow, in the order a case tends to run.

1 Reviewing an initial complaint and structuring the investigation plan

For turning a referral or complaint into a structured plan capable of forming the basis of an IMD.

Give it: the complaint or referral, and anything already actioned. **Then append the grounding rules.**

THE PROMPT

You are assisting a UK investigator reviewing an initial complaint. Below is an anonymised summary.

Produce a draft investigation plan under these headings:

1. What is alleged, stated neutrally, separating fact from assertion
2. Offences or breaches potentially engaged, and for each the elements to be proved
3. For each element, the categories of evidence capable of proving it
4. Reasonable lines of enquiry, ranked by priority and by risk of material being lost
5. Lines of enquiry pointing AWAY from wrongdoing, or towards an innocent explanation
6. Material likely to exist, and where it is likely to be held
7. Immediate actions and preservation steps
8. Gaps in what I have told you, listed as questions

Anything not in my summary belongs in section 8 as a question, never in the body as an assumption.

COMPLAINT SUMMARY:
[paste anonymised summary]

THE CHECK

Verify every offence and element against the statute itself or with your legal team. Models misstate the elements of UK offences and occasionally invent them.

WATCH-OUT

Section 5 is the one that matters. The CPIA Code duty is to pursue all reasonable lines of enquiry, including those pointing away from the suspect. An output that only builds the case is an incomplete plan.

2 Identifying lines of enquiry from material, and feeding the IMD

For working through material item by item and extracting what each one actually generates.

Give it: one category of material at a time, saying what it is and where it came from. **Then append the grounding rules.**

THE PROMPT

Below is anonymised [material type: witness account / financial records / communications data / inspection report].

Produce a table with these columns:

- Fact or assertion arising, with the words it comes from
- STATED in the material, or INFERRED by you
- The line of enquiry it generates
- What that enquiry could prove or disprove
- Whether it appears consistent or inconsistent with the allegation
- Material needed to pursue it, and where it may be held

Then list separately any line of enquiry pointing away from wrongdoing, or towards an innocent explanation.

Return the table in a form I can paste into a document.

MATERIAL:
[paste anonymised material]

THE CHECK

Every row must trace to words in the material. Test the INFERRED rows hardest — those are the ones that will not survive scrutiny.

WATCH-OUT

This generates candidate lines of enquiry. Whether each is *reasonable* in the context of this case is your judgement, and reasonableness is what a court will examine. Run it across each material type separately; the output is a feed into your plan, not the plan.

3 Drafting a digital strategy for the IMD

For structuring the digital strategy Annex A expects, before it goes to the prosecutor.

Give it: a description of the data sources, their volume and date range, and the issues in the case — not the data itself. **Then append the grounding rules.**

THE PROMPT

I am preparing a digital strategy for an investigation involving a large volume of digital material. It will be recorded in an Investigation Management Document (IMD), which the prosecutor will use to prepare the Disclosure Management Document served on the court and defence, so it must be capable of being explained to both.

Using the issues below, draft a strategy covering:

1. The issues in the case the search must address
2. The reasonable lines of enquiry the strategy pursues
3. A proposed scoping exercise before full review
4. Categories of data to target, each tied to a stated issue
5. Proposed search terms and date ranges, each tied to the issue it addresses
6. Material NOT proposed for examination, and why
7. What to record at each stage to evidence the approach
8. Points at which the strategy should be reviewed

Do not propose any search that is not tied to a stated issue. Flag anything that appears disproportionate to the issues.

ISSUES AND MATERIAL:

[describe the sources, volume, date range and issues]

THE CHECK

Your strategy goes in the IMD and is agreed with the prosecutor, who carries it into the lawyers' Disclosure Management Document and from there to the court and defence. The prosecutor signs it off; the tool does not.

WATCH-OUT

Annex A places the strategy with the person in charge of the investigation, and requires search terms and key judgements to be recorded. Annex A does expressly accept search tools, algorithms and predictive coding as a method of examining material — but the reasoning behind the strategy has to be yours.

4 Planning a PEACE interview from the case material

For deriving interview aims, topics and question structure from the material itself. Prompt 8 will build the timeline if you do not already have one.

Give it: the case summary, the offences under consideration, a timeline, and the key material. **Then append the grounding rules.**

THE PROMPT

You are assisting a UK investigator planning a PEACE-model interview. Below is a case summary, the offences under consideration, a timeline, and the key material I hold.

Produce:

1. Aims and objectives, each stated so I can tell afterwards whether it was met
2. The points to prove, and against each, the material I hold that bears on it
3. Topic areas in a logical order drawn from the material, with the reason for that order
4. Per topic: open-ended questions to obtain the account, then specific-closed to clarify and probe
5. Where each exhibit should be introduced in the sequence, and why at that point
6. Gaps — points to prove I hold no material for, and topics the material suggests I have missed
7. Accounts I should anticipate, and what each would require me to explore

Use open-ended questions to obtain the account and specific-closed only to clarify. No leading, forced-choice, multiple, repetitive or pressuring questions.

CASE SUMMARY, TIMELINE AND MATERIAL:

[paste anonymised]

THE CHECK

Read every question aloud for leading or oppressive phrasing before taking it into the room. Item 6 is the output worth most — test the gaps it identifies against your own review of the material rather than accepting them.

WATCH-OUT

College of Policing guidance sequences open-ended questions to obtain the account, then specific-closed to clarify — commonly taught as the funnel, though that is a training term rather than official terminology. The plan is a structure to open with, not a script: follow the account you receive. Interviews under caution engage PACE Code C.

5 Building an initial open-source research strategy

For settling your approach, and your audit trail, before any research begins.

Give it: the subject type and what you are trying to establish. Planning only — no results.

THE PROMPT

I am planning open-source research for a lawful UK investigation.

Subject of the research: [a company / a vehicle / a publicly available record]
What I am trying to establish: [state it]

Produce a research strategy setting out:

1. Categories of open source worth considering, in the order to approach them, and the issue each step serves
2. What each category is reliable for, and what it is not
3. What to capture and record at each step to preserve continuity and an audit trail
4. The point at which research on an individual would move from general to systematic, and would therefore require an authorisation to be considered
5. What not to do

Do not perform any searches. Do not suggest deception, false identities, account creation, or access to material that is not publicly available.

THE CHECK

Assess every suggested source against your own authority position before approaching it.

WATCH-OUT

Repeated or systematic viewing of an individual's online presence may require a directed surveillance authorisation and, for local authorities, magistrates' approval under s.32A RIPA. Item 5 is a prompt for your judgement, not a substitute for it.

6 Reviewing unused material and signposting for disclosure

For reading an item of unused material and identifying what the disclosure officer needs to turn their mind to.

Give it: the item of unused material, and the issues in the case. **Then append the grounding rules.**

THE PROMPT

You are assisting a UK disclosure officer. Below is an item of material from a criminal investigation.

The issues in the case are: [state the issues]
The prosecution case is, in summary: [one or two lines]

Produce:

1. What this item is and where it came from, taken from the material itself
2. An accurate factual summary of its contents
3. Anything that may point TOWARDS the suspect, quoted with its location
4. Anything that may point AWAY from the suspect, or that may assist a defence, quoted with its location
5. Anything that appears inconsistent with the prosecution case as I have described it
6. Anything appearing personal, third-party, legally privileged or otherwise potentially sensitive, flagged for my consideration
7. A suggested neutral schedule description of under 40 words

For items 3 to 6, flag the point and explain why it may matter. Do not decide whether anything is relevant, sensitive or disclosable — those decisions are mine.

MATERIAL:
[paste the item]

THE CHECK

Read the item yourself and check every quotation. The output is a signpost to material you must assess, not an assessment. You apply the relevancy test, you decide sensitivity, and you apply the disclosure test.

WATCH-OUT

Under s.7A CPIA 1996 and the AG's Guidelines on Disclosure 2024 the duty is continuing and the disclosure officer's declaration is personal. The tool may draw your attention to a fact; it cannot tell you whether that fact undermines the prosecution case or assists the case for the accused.

7 Summarising a single document

For finding your way around one long document and deciding where to read properly.

Give it: the document, and the issue you want it read against. **Then append the grounding rules.**

THE PROMPT

Summarise the document below in four parts:

1. What this document is, who created it and when – taken from the document only
2. A 150-word overview
3. The points most relevant to [state your issue], each with a direct quotation and its page or paragraph reference
4. Anything appearing to contradict or undermine [state your issue], with quotations

Support every point with a direct quotation. If you cannot, do not make the point.

DOCUMENT:

[paste anonymised text]

THE CHECK

Open the document and read every quoted passage in context. A summary you have not spot-checked establishes nothing.

WATCH-OUT

Triage, not review. It indicates where to look. Never rely on it to establish that something is *absent* from a document — that is precisely the failure mode.

8 Building a case summary and timeline across documents

For synthesising several documents into a chronology and summary you can work from.

Give it: the documents, each labelled so you can trace an entry back to its source. **Then append the grounding rules.**

THE PROMPT

Below are several anonymised documents relating to one investigation, each labelled.

Produce:

1. A chronological timeline with columns: date (DD/MM/YYYY), time (24hr), event, source document, confidence (STATED / INFERRED / UNCLEAR)
2. A case summary of no more than 500 words in neutral factual language
3. Inconsistencies or conflicts between the documents, with the conflicting passages quoted
4. Gaps in the chronology – periods where something appears to be missing
5. Topics arising that may need to be covered in interview

Return the timeline in a form I can paste into a document.

DOCUMENTS:

[paste anonymised documents, each clearly labelled]

THE CHECK

Every timeline entry must trace to a source document. The conflicts list is the most valuable output and the one to verify personally.

WATCH-OUT

This is where volume creates risk. The summary is a navigation aid to material you must still read — it is not the case, and it is not a substitute for reading the documents.

9 Rewriting a summary for a specific audience

For putting a factual summary in front of a committee, a panel or a senior manager.

Give it: your own finished factual summary, and who it is for. **Then append the grounding rules.**

THE PROMPT

Below is a factual summary written for investigators. Rewrite it for [audience – a licensing committee / a panel / a senior manager / a lay reader].

Structure:

- A one-paragraph summary
- Key findings as short bullets
- Decisions or actions required, clearly stated

Rules:

- Keep every fact exactly as written. Do not add, remove, soften, strengthen or reorder any fact
- Do not add connecting statements, conclusions or inferences that are not in my text
- Remove jargon and acronyms, or explain them on first use
- Finally, list every change you made that goes beyond wording

SUMMARY:

[paste anonymised summary]

THE CHECK

Read the output alongside your original. Models routinely "improve" text by introducing causal or connective claims that were never there — the closing list is your check on exactly that.

WATCH-OUT

Anonymise first. Structure and tone are the only things being altered; the facts are not open to editing.

10 Building a slide deck to present analytical findings

For presenting analysis to a committee, a case conference or a management board.

Give it: your analysis or figures, the audience, and the number of slides. **Then append the grounding rules.**

THE PROMPT

I need to present the analysis below to [audience] in [number] slides.

Produce a slide-by-slide outline. For each slide give:

- A title written as the point being made, not as a label
- Three or four bullets in plain English
- What the visual should be (chart type, table, timeline) and exactly what it should show
- What I should say that is not on the slide
- The source of every figure on the slide

Rules:

- One point per slide
- Use only figures present in my analysis. Do not calculate, estimate, round or extrapolate anything I have not given you
- Flag any figure that would mislead if presented without its caveat
- Finish with a slide setting out the decisions required

ANALYSIS:

[paste anonymised analysis or figures]

THE CHECK

Check every figure on every slide against your source data. A transposed number in a deck is harder to spot and travels further than one in a report.

WATCH-OUT

If you are generating the deck in Copilot from a document in your tenant, check what it drew on and what it left out. Presentation choices — scale, comparison, chart type — are argument rather than decoration, and you must be able to justify each of them.

Where to go next

If this has been useful, three things are worth knowing about.

Keep the pack working for you

Each of the following is built on the same principle: AI assists, the investigator decides, and the decision is recorded.

The Investigator Bulletin — free, monthly

Practical updates on investigative practice, legislation and case law for UK public sector investigators, written by practitioners.

bdgtrainingconsultancy.co.uk/investigator-bulletin

The full Prompt Handbook — in preparation

Sixty-plus prompts across the investigative workflow, each with its legal watch-out: scoping, open source, chronologies, statements and exhibits, disclosure, interviews, decision logs and reporting. Bulletin subscribers are notified first.

AI governance for investigation teams

Policy, decision-log and oversight templates for managers who need a documented position on AI use in investigations rather than an informal one. Available as a standalone pack or delivered in-house.

Training

Investigation and Decision Making · Statements and Exhibits · PACE · Disclosure · Court Skills · Open Source · RIPA (Applicant, Authorising Officer, CHIS Handler and Controller) · Covert Investigations. Delivered classroom, virtual, blended or in-house.

bdgtrainingconsultancy.co.uk

A closing observation

The question is no longer whether investigators will use AI; the majority already do. The question is whether they are doing so in a manner that could be explained to a court, an auditor or an information governance review — and whether anyone has shown them how. That is a training matter rather than a technology one, which is rather the point.

The UK Investigator's AI Starter Pack · Edition 1 · August 2026

BDG Training Team · info@bdgtrainingconsultancy.co.uk · www.bdgtrainingconsultancy.co.uk



Sources referred to: AI Playbook for the UK Government (DSIT) · Police use of artificial intelligence factsheet (Home Office) · IPCO, IPCO's *Scope of Interest in AI*, 26 March 2025 · Equality Act 2010 · Government Security Classifications Policy (Cabinet Office, current version August 2024) · Attorney General's Guidelines on Disclosure 2024, effective 29 May 2024, and Annex A (Digital Material) · Criminal Procedure and Investigations Act 1996, ss.7A and 26, and the CPIA Code of Practice · Police and Criminal Evidence Act 1984, s.76 and Code C · College of Policing Authorised Professional Practice on investigative interviewing · Regulation of Investigatory Powers Act 2000, s.32A, and the Covert Surveillance and Property Interference Code of Practice · ICO consultation on draft guidance on automated decision-making and profiling, 2026, and the Data Protection Act 2018 (Code of Practice on Artificial Intelligence and Automated Decision-Making) Regulations 2026 · Microsoft Learn documentation on Microsoft 365 Copilot privacy, data protection and auditing · Skillcast, *AI Adoption in the Workplace: The UK's Governance Gap*, July 2026 (a vendor-commissioned online panel survey of 500 respondents; figures are indicative).

This guide is provided for general professional development. It does not constitute legal advice and should not be relied upon as such. It does not replace your organisation's own policies on artificial intelligence, information governance or data protection — consult those first, together with your Data Protection Officer and legal team, on any live matter. Platform capabilities, legislation, guidance and regulatory expectations in this area are developing quickly; content is current as at August 2026 and platform behaviour should be confirmed with your IT service.

This document may be shared in full within your organisation. Please do not extract or resell its contents.