ULLR INTELLIGENCE™

The Desk Investigator's Field Manual

OSINT, tradecraft and compliance for UK private investigators

Hunt in the open. Leave no trace. Stay on the right side of the law.

THE FULL FIRST EDITION HAS

40 chapters, including **8** playbooks and **4** case studies, plus **13** templates

This free sample contains

Chapter 3 · The UK Legal & Ethical Framework
Chapter 26 · The Running File
Chapter 30 · Playbook 4: Corporate & Director Due Diligence
Case B from Chapter 35 (Case Studies)
A worked template from Appendix C (Ready Templates)
One page of The UK OSINT Tool Index

FIRST EDITION · OCTOBER 2026 · FREE SAMPLE PDF

FREE SAMPLE

Chapters 3, 26 and 30 · Case B · a worked template · one Tool Index page

The Desk Investigator's Field Manual

First Edition, October 2026 · Version 1.0

© 2026 Ullr Intelligence Ltd. All rights reserved.

Ullr Intelligence Ltd · Registered in England and Wales, company no. 17117362 · Registered with the Information Commission (still known as the ICO), ref. ZC197792

This free sample may be shared, as long as it is complete and unchanged. The full manual is licensed, not sold: see https://ullrintelligence.co.uk/licence. Cross-references to other chapters, templates and appendices point to the full First Edition.

> **READ THIS FIRST**
>
> This manual is an educational and operational reference, not legal advice. The publisher is not your solicitor and does not act for you.
>
> Every technique here must be carried out under a documented lawful basis and within the law of the jurisdiction you operate in. You, the investigator, are solely responsible for your own compliance with the UK GDPR, the Data Protection Act 2018, the Computer Misuse Act 1990 and all other applicable law.
>
> Tools, prices, URLs and the law change constantly. Everything here is a starting point to verify at source. The publisher's liability is limited to the price you paid, as set out in the licence terms (https://ullrintelligence.co.uk/licence). Nothing limits or excludes liability that cannot be limited or excluded by law, including your statutory rights as a consumer.
> The case studies and worked examples are fictional composites. Names, companies, numbers and places are invented; any resemblance to real people or businesses is coincidental.
> Listing a tool is not an endorsement or a recommendation to buy it.

Currency note. Legal and regulatory facts in this edition were checked against official sources on 20/10/2026 (corrections checked 27/10/2026), including the Data (Use and Access) Act 2025 commencements, the Information Commission's replacement of the Information Commissioner on 30/09/2026, Companies House identity verification, the UK Sanctions List and the SIA fee. Each chapter shows the date it was last reviewed. Tool prices are indicative: confirm them on the vendor's own page before you spend or send identifiers.

Contents

Contents of the full manual. Page numbers refer to the full First Edition; this free sample contains Chapters 3, 26 and 30, Case B from Chapter 35, a worked page from Appendix C and one page of the Tool Index.

About the Author v
Licence, Copyright & Updates vi
Notices vii
About this Edition viii
Quick Start: Before Your First Instruction ix
How to Use This Manual x

PART I · Foundations 1
1 · What Desk-Based OSINT Investigation Actually Is 2
2 · The Investigator's Mindset & the Ground Rules 3
3 · The UK Legal & Ethical Framework 4
4 · Client Intake & Lawful Case Setup 8
5 · Where Your Identifiers Go: Vendors, Transfers & AI 9

PART II · The Desk, the Machine & the Tradecraft 12
6 · Your Desk & Environment 13
7 · Managed Attribution & OPSEC 14
8 · Virtual Machines & Your OSINT Lab 16
9 · Browser Tradecraft 17
10 · Evidence Handling & Chain of Custody 18
11 · Case Management in Your Notebook 20

PART III · The Tool Library 21
12 · Search, Dorking & Archives 22
13 · UK People & Identity Tracing 23
14 · Corporate & Director Intelligence 24
15 · Social Media & Username Intelligence 25
16 · Email, Phone & Digital Footprint 26
17 · Image & Video Intelligence 27
18 · Domain, IP & Infrastructure 29
19 · Breach & Dark-Web Intelligence (Tier 3) 30
20 · Financial & Asset Intelligence 32
21 · Legal, Court & Public Records 33
22 · Geospatial Intelligence 35
23 · Link Analysis & Professional Platforms 36
24 · AI-Assisted OSINT 37
25 · Monitoring & Alerting 38

PART IV · The Playbooks 39
26 · The Running File: Identifiers, Searches, Exhibits, Leads, Findings 40
27 · Playbook 1: Your Very First Case 42
28 · Playbook 2: Locating a Person / Skip Trace 43
29 · Playbook 3: Pre-Employment & Tenant Screening 44
30 · Playbook 4: Corporate & Director Due Diligence 45
31 · Playbook 5: Asset Tracing 46
32 · Playbook 6: Adverse Media & Reputation 47
33 · Playbook 7: Online Profile / SOCMINT Investigation 48
34 · Playbook 8: Verifying an Image or Video 49
35 · Case Studies: Four Fictional Matters 50

PART V · Standards, Wellbeing & Growth 54

36 · Writing the Report....55
37 · Disambiguating Common Names....57
38 · Wellbeing & the Hard Edges....58
39 · The Upgrade Ladder: Your Investment Path....59
40 · Keeping This Manual Alive....60
REFERENCE · Appendices....61
Appendix A · Google Dork Cheat-Sheet....62
Appendix B · Quick Tool Matrix....63
Appendix C · Ready Templates....65
Appendix D · Glossary....92
Appendix E · Quick-Reference Cards....94

3 · The UK Legal & Ethical Framework

Last reviewed 27/10/2026

This is the most important chapter in the book. Tool capability is never the same as lawful permission. Read it slowly; everything that follows depends on it.

You are almost always a "controller"

If you decide why and how personal data is processed, you are a data controller under the UK GDPR and the Data Protection Act 2018, with all the duties that brings. Sometimes you act on a client's detailed instructions and are a processor; occasionally you and the client decide together and are joint controllers (Article 26). Your role is a question of fact, not preference, and you must have a lawful basis before you process anything. Collecting data about someone from other sources normally means telling them (Article 14), unless you can show they already have the information (Article 14(5)(a)). Otherwise you need an exception: notice would be impossible or involve disproportionate effort (Article 14(5)(e)), or would seriously impair the purpose, as in most covert work (Article 14(5)(f)), each with the safeguards Article 14(7) requires, including making the information publicly available; or a DPA 2018 Schedule 2 exemption for crime or legal proceedings. Record which one applies on the LIA (C11).

The principles, in brief

Lawfulness, fairness and transparency · purpose limitation · data minimisation · accuracy · storage limitation · integrity and confidentiality (security) · accountability. Every one of them argues for the same behaviour: take only what you need, for a clear purpose, keep it accurate and secure, and be able to justify it.

The seven lawful bases, and the one you'll usually use

Consent · contract · legal obligation · vital interests · public task · legitimate interests · and, since 05/02/2026, **recognised legitimate interests** (Article 6(1)(ea) UK GDPR, added by section 70 of the Data (Use and Access) Act 2025). For most investigative work the workhorse is still ordinary legitimate interests: yours, the client's, or a third party's. It needs a documented three-part test, the LIA:

1. **Purpose.** Is there a real, specific, legitimate interest being pursued?
2. **Necessity.** Is this processing actually needed to achieve it, or would less do?
3. **Balance.** Do your interests override the individual's rights, freedoms and reasonable expectations? If not, you stop.

> **IN PLAIN ENGLISH**
> Legitimate interests in one sentence: "I have a genuine reason, I'm taking only what I need for it, and a reasonable person wouldn't be shocked." Write all three down before you start. A blank LIA is a red flag in any audit; the template is in Appendix C.

Recognised legitimate interests: narrower than they sound

Annex 1 to the UK GDPR lists a closed set of purposes that need no balancing test: answering a request from a body carrying out a public task; national security, public security and defence; emergencies; detecting, investigating or preventing crime, or apprehending or

prosecuting offenders; and safeguarding vulnerable individuals. Necessity still applies. The crime condition can matter in fraud work, but it does not cover general due diligence, screening, or tracing for a civil debt. If you rely on it, record which Annex 1 condition applies and why the processing is necessary. Special-category and criminal-offence data still need their own conditions.

Special-category and criminal-offence data

Some data is higher risk: race or ethnicity, health, sex life or sexual orientation, religion or philosophy, political opinions, trade-union membership, genetics and biometrics (which can include facial-recognition matching). Criminal-offence data covers allegations and convictions. Processing any of it needs an additional condition and almost always a DPIA. The conditions a PI most often uses are legal claims (Article 9(2)(f) UK GDPR; for criminal-offence data, DPA 2018 Schedule 1 para 33) and preventing, investigating or detecting unlawful acts, where asking for consent would prejudice that and there is a substantial public interest (Schedule 1 para 10); record the condition on the LIA (C11), and where Schedule 1 requires it, keep an appropriate policy document on file. Note how quickly ordinary requests land here: "run his face" or "is he a criminal?" are special-category and criminal-offence processing respectively.

LEGAL LINE

"Blagging" is a crime. Knowingly or recklessly obtaining, disclosing or procuring personal data without the controller's consent (pretexting) is an offence under section 170 of the Data Protection Act 2018.

Phoning a bank, utility, GP, landlord or employer while pretending to be the subject (or someone authorised by them) to extract their data is a criminal act, however good the cause. This manual will never teach it, and you must never do it. If the only way to get something is to deceive a human into releasing it, the answer is: you don't get it.

LEGAL LINE

Don't touch what isn't yours. Accessing any account, inbox, device or system you are not authorised to use (guessing or reusing someone's password, getting into an email or social account, probing or exploiting a server) is an offence under the Computer Misuse Act 1990.

Passively viewing a public page is fine. The moment you authenticate, bypass, or poke at something private, you have crossed into the CMA. There is no "investigative purpose" exception.

PECR: when you communicate

If your work ever extends to outreach or email, the Privacy and Electronic Communications Regulations apply alongside the UK GDPR. This matters most when you use email-finding tools: keep discovery strictly separate from contact, and never repurpose discovered addresses for marketing, or as a starting point for unrelated enquiries.

LEGAL LINE

Don't become the stalker. A course of conduct amounting to harassment (repeated, oppressive monitoring or contact that a reasonable person would find alarming or distressing) is both a civil wrong and a criminal offence under the Protection from Harassment Act 1997.

Persistent, intensive online surveillance of an individual can cross this line even from a desk. Necessity, proportionality and a genuine lawful purpose are what keep you an investigator rather than an offender.

Article 8 and reasonable expectation of privacy

Even public data can carry a privacy expectation, especially once you aggregate scattered details into a profile. "But it was public" is not a complete defence. Article 8 binds public authorities; against a private investigator the claim is the tort of misuse of private information, alongside harassment. The question is always whether your collection was necessary and proportionate to a legitimate purpose.

The ABI Code: your best credibility move

In October 2024 the ICO approved the Association of British Investigators' UK GDPR Code of Conduct for Investigative & Litigation Support Services: the first sector-owned UK GDPR code under Article 40. Its independent monitoring body, SSAIB, began accepting applications in May 2026. The Code is voluntary and open to non-members, gives you a ready-made, sector-specific compliance framework, and the regulator will take adherence into account in any enforcement action. For a new desk-based PI, signing up to it is one of the strongest signals of professionalism you can send a client or a court.

The regulator is now the Information Commission

On 30/09/2026 the Information Commission took over from the Information Commissioner. It is a body corporate run by a board rather than a single Commissioner; its existing powers continue. The regulator is still known as the ICO; ico.org.uk is unchanged. Name the Information Commission (the ICO) in your privacy notice and engagement letter.

RIPA and IPCO: the powers you do NOT have

The Regulation of Investigatory Powers Act 2000 governs covert surveillance by public authorities (in Scotland, devolved bodies use the Regulation of Investigatory Powers (Scotland) Act 2000); IPCO oversees those statutory powers. As a private investigator you do not acquire any of them simply by being instructed. If a public body engages you, obtain written confirmation of their RIPA position, authorisation status and the permitted activity before any covert work, and get legal advice. Never assume a client's powers are yours.

SIA licensing: where it bites

Private investigation is not, at present, a licensable activity anywhere in the UK: the statutory licensing scheme for PIs was never brought into force, so the work is not regulated by statute. But if you also undertake regulated security work (public-space CCTV surveillance, door supervision, close protection, guarding), you need the relevant SIA licence for that activity. The SIA application fee became £204 on 01/04/2026 when the temporary £20 rebate ended, and the licensing criteria tightened on 01/12/2025. Assess your obligations by activity, not by job title.

Scotland and Northern Ireland

The UK GDPR, the Data Protection Act 2018, the Computer Misuse Act and the UK sanctions regime apply across the UK. Other things differ. Scotland has its own courts, land register, insolvency register and charity regulator, and stalking is a separate offence under section 39 of the Criminal Justice and Licensing (Scotland) Act 2010. Northern Ireland has the Protection from Harassment (Northern Ireland) Order 1997 and the Protection from Stalking Act (Northern Ireland) 2022, and its own land, insolvency and charity registers. When a subject or a source is in Scotland or Northern Ireland, use the local registers in Part III, and take local advice if a step turns on the criminal law.

The housekeeping that makes you legitimate

- Pay the annual data protection fee to the Information Commission (the ICO).
- Carry professional indemnity insurance (and public liability) appropriate to investigative work.
- Consider membership of the ABI or WAPI for standards, network and credibility.
- Maintain contemporaneous case logs (the running file, Chapter 26).
- Keep client instructions, lawful-basis assessments and DPIAs on file for every matter.

> **NOTE**
> None of this is box-ticking. It is what lets you say, under scrutiny: "Here is my lawful basis, here is what I did, and here is why it was necessary and proportionate." That sentence is what you'll point to if your work is challenged, so build every case so you can say it.

Minimum written policies

You do not need a fat manual before you take work. You do need these five, written down, dated, and followed.
Privacy notice: who you are, what you collect, the basis, how long you keep it, how to complain to you and to the Information Commission, and your data protection fee registration number.
Retention and destruction: default period per matter, how you destroy, what triggers a hold.
Information security: encrypted devices, who can see a matter file, what happens if a laptop is lost, which tools may receive identifiers.
Lawful methods: public sources only; no blagging; no unauthorised access; no subject contact unless the schedule says so; biometric and Tier 3 gates.
Complaints: where a client or a data subject writes, and how long you take to answer. Since 19/06/2026 the law requires this for data protection complaints from data subjects: make it easy to complain to you (for example an electronic complaint form), acknowledge each complaint within 30 days, and without undue delay look into it, keep the complainant informed and tell them the outcome (s.164A DPA 2018, inserted by s.103 DUAA). Acknowledging a client's service complaint within 30 days is good practice, not a legal duty.
Keep a register of processing (what you actually do) and a vendor list of every service that receives identifiers (Chapter 5). Five short pages you follow beat fifty pages you do not. A subject may ask what you hold on them: answer a subject access request within one month after a reasonable and proportionate search, apply only the exemptions that fit (crime, legal proceedings or legal professional privilege, DPA 2018 Schedule 2), and log the decision.

26 · The Running File: Identifiers, Searches, Exhibits, Leads, Findings

Last reviewed 27/10/2026

This chapter is the one that is missing from most first cases. The playbooks that follow only work if you run paper in this order. Tools do not replace it.

The objects are not the same

Identifier. A string you are allowed to put into a source: a name, an alias, an email, a phone, a handle, a company number, a URL. It lives on the Identifiers register before it lives in a search box. If it is not on that page, you do not search it.
Search. One action against one identifier (or one bounded query). One row in the Search log. The result of a search is a lead, even when the page looks like a bullseye.
Exhibit. A file you captured while searching: PDF, screenshot, export. Hash it. Give it a number. One exhibit may support several later findings. Do not recapture the same page three times because three findings mention it.
Lead. Something the search suggested that might matter. It lives on the Leads register with a status: open, discarded, or promoted. Most leads die. That is competence, not laziness.
Finding. A claim you are prepared to put in the report. It gets a verification block, which you write and sign, and a grade on the six-grade scale (Chapter 36). Until then it is not a finding, however pretty the screenshot.
Follow-up. A task you could not finish during the search: a login wall, a paid check that needs the client's approval, a portal form, a page that would not load. It has a URL or a portal name, or it is not a follow-up.

The flow, every time

Write the hypothesis and the authorised identifiers. LIA (and a DPIA, if Chapter 4 calls for one) or consent already on file.
Capture as you search. Row in the Search log first, exhibit second, lead third. Not the other way around.
Close leads in batches. Discard namesakes and tool-ticks. Promote only what the purpose needs.
Open a verification block only for promoted leads. Check the primary source before you grade anything Confirmed; two independent sources that agree make it Corroborated. Sign it.
Decisions log only when you judge: stop, refuse a tool, change a name on the cover, carry an empty row.
The follow-up list is the only to-do you should have to read. If the list is empty, write the report.

What "enough" looks like

You stop when the hypothesis is answered or honestly exhausted, not when every similar name on the platform has been opened. Two independent anchors beat fifty thin hits. One breach fact is recorded once. Registration ticks stay leads until the account is attributed.

Worked rows (fictional: copy the shape, not the facts)

Search #014 | 03/03/2026 10:15 GMT (+00:00) | company name "Brindle & Vane Ltd" on Companies House | Result: active company, two directors, one registered charge | Ex-07 | Next: pull the charge; check both directors' other appointments.
Search #015 | 03/03/2026 10:32 GMT (+00:00) | the director's appointments page on Companies House | Result: three appointments at companies dissolved in 2024–2025, all at the same address | Ex-08 | Next: check The Gazette for strike-off notices.

Lead L-06 | from #015 | one director held appointments at three companies dissolved at the same address | second source: The Gazette strike-off notices, captured as Ex-09 | promoted to F03.
Finding F03 | A current director of Brindle & Vane Ltd was a director of three companies dissolved in 2024–2025 | Confirmed (the director's Companies House appointments page, which shows each company as dissolved, the primary source; The Gazette agrees) | Ex-07, Ex-08, Ex-09 | signed.
Do not also open a separate finding for each of the three companies, each saying "director linked to a dissolved company": that is the same fact three times. (In Case B, draft F02 stated the same fact again and was merged into F03 before issue: see C6. Brindle & Vane Ltd is an invented company.)
The ready forms for every object in this chapter are Appendix C. Duplicate those pages per matter. After C13, Appendix C shows C1 to C8 and C13 filled in for Case B (Chapter 35).

30 · Playbook 4: Corporate & Director Due Diligence

Last reviewed 27/10/2026

This is the desk investigator's strongest game, thanks to UK corporate transparency. Whether for investment, partnership, a supplier, an acquisition or KYC, the route is well-trodden.

1. Map the entity. Companies House: status, incorporation, officers, PSCs and their identity verification status against each person's due date, accounts, charges, filing history.
2. **Map the people.** Officers and PSCs → cross-directorships → recurring names → the wider cluster of companies they touch.
3. **Assess financial health.** Accounts trend, charges (who they owe), CCJs, Creditsafe/Red Flag alerts, insolvency history.
4. Check integrity flags. Disqualified directors, dissolved/phoenix patterns, FCA authorisation if regulated, the UK Sanctions List and the Russia financial and investment restrictions list, adverse media.
5. **Test the ownership reality.** Registered vs trading address, overseas links (OpenCorporates/ICIJ), nominee or holding structures.
6. **Synthesise a structured profile (structure, control, standing, red flags), every point** evidenced and dated.

IN PLAIN ENGLISH

"Due diligence" / KYC means checking who you're really dealing with and whether they're sound, before money or trust changes hands. The deliverable is a clear, evidenced picture, not a verdict.

TRADECRAFT

Watch for the "phoenix" pattern: a series of similar companies dissolved owing money, then reborn under new names with the same directors. Cross-directorship mapping exposes it fast. And remember: company data is self-reported and can be gamed, so corroborate the claims that matter; the absence of a red flag is not proof of integrity.

Running-file notes

Company number is the identifier that matters. Names are how you get to the number. Once you have the number, every search row should carry it.

Companies House live record first. Officer names become new identifiers on the register before you search the person. Mapping officers and PSCs across registers is data matching: have the LIA and a DPIA (C12) on file first, as in Case B (Chapter 4). An aggregator page is a lead. Companies House is the primary.

If the PSC layer is silent, say so. Do not infer a beneficial owner from a rumour.

35 · Case Studies (extract: Case B)

Last reviewed 27/10/2026

> **NOTE**
> Every person, company, address and date in this chapter is invented. The cases are composites built to show method, decisions and grading. They describe no real matter.

Case B · A new supplier with a short history

Instruction. A manufacturer is about to pay a large deposit to Brindle & Vane Ltd for packaging, and asks whether it is an established, solvent supplier able to take a large order. Matter MAT-2026-014, opened 02/03/2026.

Tier and basis. Corporate due diligence (Chapter 30), Tier 1 only. The basis is the client's legitimate interest in knowing who it is paying, with an LIA (C11) and, for matching the directors across registers, a DPIA-lite (C12): residual risk Low, no full DPIA. The directors are searched in their company roles only: their private lives are outside the purpose. The Individual Insolvency Register is in scope too: an undischarged bankrupt may not act as a director without the court's permission (Company Directors Disqualification Act 1986, s.11).

What you ran. Thirty Search rows and twenty-three exhibits, 02/03/2026 to 04/03/2026: the quotation, website, domain and Street View; Companies House (profile, officers, appointments, PSC register, charges and the Disqualified Directors Register); The Gazette, for the three dissolved companies; the UK Sanctions List and the Russia list, screened again on the morning of issue, when The Gazette was also searched for insolvency notices on the company and the Individual Insolvency Register on both directors; adverse media in two engines on the company and on each director in a company role; and the mail-forwarding provider's own website.

What you found. The hypothesis is not supported as stated. The company is active but eleven months old (F01). One director, who is also the only PSC, was a director of three companies dissolved in 2024–2025 at the same address: Confirmed (F03 and F09; F03 is the worked finding in Chapter 26). Companies House shows the other director's identity as verified and this director's verification as not yet due; the report states that as a fact about the register (F10). No sanctions match on either list, and neither director is disqualified: Not found, dated (F04, F11). No insolvency notice for the company in The Gazette, and neither director on the Individual Insolvency Register: Not found (F12). The trading address is a mail-forwarding service: Corroborated by Street View and the provider's own website (F05). No adverse media: Not found (F06).

What you did not do, and why. The FCA register, because packaging supply is not a regulated activity: Not checked (F08). No credit report or County Court Judgments search: the client declined both paid checks, so the report says solvency could not be assessed. The Individual Insolvency Register covers England and Wales only; the Scottish and Northern Ireland registers were not searched, as nothing in the file points to either. No search of the directors' private lives, homes or social media; a personal phone number seen in a forum post was struck from the register as out of scope and not searched. No contact with the company.

Lesson. Answer the hypothesis first, then give the facts and the grades. None of this proves dishonesty: the report recommends staged payments and doesn't say "phoenix fraud". The whole running file for this case, filled in, is the worked example at the end of Appendix C.

APPENDIX C · WORKED EXAMPLE · C5 *From Appendix C of the full manual: worked example (fictional)*

C5 · Verification log

One block per finding you will put in the report. You write it. You sign it. Three of the eleven findings are shown; draft F02 was merged into F03 (C6).

Finding F03

Claim	A current director of Brindle & Vane Ltd was a director of three companies dissolved in 2024–2025.
Draft grade	Confirmed
Primary source	Companies House: Rowan Example's appointments page, which shows each company as dissolved, 03/03/2026 10:32 GMT (+00:00)
Second source	The Gazette: first and final strike-off notices for all three, 03/03/2026 10:48 GMT (+00:00)
Exhibits	Ex-07, Ex-08, Ex-09
Search rows	#014, #015, #016
What would change the grade	An officer record showing a different person of the same name. Checked: same name, same month and year of birth, same correspondence address.
Signed + date	A. Example, 03/03/2026

Finding F04

Claim	Neither Brindle & Vane Ltd nor either of its two directors appears on the UK Sanctions List or on the Russia financial and investment restrictions list.
Draft grade	Not found
Primary source	UK Sanctions List search, 03/03/2026 11:35 GMT (+00:00); run again 04/03/2026 08:55 GMT (+00:00)
Second source	Not needed for Not found. The Russia list was searched too: it is a separate list, not a second source.
Exhibits	Ex-13, Ex-14, Ex-21
Search rows	#020, #021, #028
What would change the grade	A designation after 04/03/2026. Screen again before any later payment.
Signed + date	A. Example, 04/03/2026

Finding F05

Claim	The trading address on the supplier's quotation is a mail-forwarding service.
Draft grade	Corroborated
Primary source	None: no register records how an address is used, so this cannot be Confirmed.
Second source	Two independent sources agree: Street View (image dated 06/2025), seen 02/03/2026 15:40 GMT (+00:00); the provider's own website, 03/03/2026 12:25 GMT (+00:00)
Exhibits	Ex-06, Ex-17
Search rows	#011 (sheet 1), #024
What would change the grade	A newer Street View image, or the provider's website, showing a different occupier.
Signed + date	A. Example, 03/03/2026

Matter ref MAT-2026-014 Date 04/03/2026 Investigator A. Example

A page from the Tool Index

Overleaf is one page of The UK OSINT Tool Index, exactly as it appears in the PDF edition: the end of category 03 (UK Companies, Directors & Beneficial Ownership) and the start of category 04 (UK Insolvency, Regulatory & Sanctions), the rows behind the director check in Chapter 30. The short codes in its cells, such as "Public register", "Consumer ToS" and "T1 gate", are explained in the key on pages 1–2 of the full Tool Index. No row on this page is shaded: elsewhere in the Index, red marks Tier 3 (gated) sources, orange a licence that bars the free tier from paid client work, yellow a restricted transfer that needs a safeguard check (or an operator that does not publish where it is), and blue an independent controller (still a restricted transfer when it is outside the UK). In the workbook (.xlsx) supplied with the Index, every row can be filtered.

Tool and URL	Tier	Jurisdiction (operator)	Cost	Commercial-use licence	Data transfer flag	Risk gate	Last verified	Notes
OpenLEIs https://openleis.com	T1	FI	Free	Consumer ToS	EEA / adequacy	T1 gate	21/10/2026	Front end on GLEIF data. Confirm at search.gleif.org.

04 · UK Insolvency, Regulatory & Sanctions

Tool and URL	Tier	Jurisdiction (operator)	Cost	Commercial-use licence	Data transfer flag	Risk gate	Last verified	Notes
Individual Insolvency Register (England & Wales) https://www.gov.uk/search-bankruptcy-insolvency-register	T1	UK	Free	Public register	UK	T1 gate	20/10/2026	Bankruptcies, IVAs, DROs (England & Wales). Search form; no bulk access.
Register of Insolvencies (Scotland, AiB) https://roi.aib.gov.uk	T1	UK	Free	Public register	UK	T1 gate	20/10/2026	Scottish sequestrations, protected trust deeds and related records from the Accountant in Bankruptcy.
Northern Ireland insolvency registers (Department for the Economy) https://www.economy-ni.gov.uk/articles/insolvency-service-do-it-online	T1	UK	Free	Public register	UK	T1 gate	20/10/2026	NI IVA register, DRO and BRO search, and the NI directors' disqualification register.
Disqualified Directors Register https://www.gov.uk/search-the-register-of-disqualified-company-directors	T1	UK	Free	Public register	UK	T1 gate	20/10/2026	Cross-check confirmed directors. Match on more than the name.
The Gazette https://www.thegazette.co.uk	T1	UK	Free	OGL v3.0	UK	T1 gate	20/10/2026	Official notices for the whole UK (London, Edinburgh and Belfast Gazettes): insolvency, winding-up, probate notices.
FCA Financial Services Register https://register.fca.org.uk/s/	T1	UK	Free	Public register	UK	T1 gate	21/10/2026	Authorisation status of firms and individuals. Also check the FCA Warning List for unauthorised firms.
UK Sanctions List search https://search-uk-sanctions-list.service.gov.uk	T1	UK	Free	Public register	UK	T1 gate	20/10/2026	The only list of UK sanctions designations since 28/01/2026 (OFSI Consolidated List closed). Screen the subject and key associates.
UK Sanctions List (publication page) https://www.gov.uk/government/publications/the-uk-sanctions-list	T1	UK	Free	OGL v3.0	UK	T1 gate	20/10/2026	Downloads and guidance for the UK Sanctions List.
Russia: persons named in relation to financial and investment restrictions https://www.gov.uk/guidance/russia-list-of-persons-named-in-relation-to-financial-and-investment-restrictions	T1	UK	Free	OGL v3.0	UK	T1 gate	20/10/2026	A separate list that is not part of the UK Sanctions List. Check it every time, alongside the UK Sanctions List.
OFSI Consolidated List (historical) https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets	—	UK	Free	OGL v3.0	UK	Reference	20/10/2026	Closed 28/01/2026. Reference only; never screen against it.

Get the full manual

The full First Edition has 40 chapters, including 8 step-by-step playbooks and 4 worked case studies, plus 13 ready templates, three quick-reference cards and UK law in plain English. It pairs with The UK OSINT Tool Index (sold separately or in the bundle): 195 entries in 24 categories, tiered, flagged and dated.

What you can buy

Field Manual (with the Fillable Templates PDF)

Tool Index (PDF, workbook and companion guide)

Manual + Index bundle

Firm licence: Manual and Index for one organisation and up to 5 named users, including contractors under its control

Current prices are on the shop page at ullrintelligence.co.uk, which carries the company's details. We sell to UK buyers only (licence clause 1.3). No VAT is added, because Ullr Intelligence Ltd is not registered for VAT. For 12 months from purchase, buyers receive updates to the product or products they bought.

Where to buy

https://ullrintelligence.co.uk
Questions, firm licences and larger teams: sales@ullrintelligence.co.uk

Ullr Intelligence Ltd · Registered in England and Wales, company no. 17117362 · Registered with the Information Commission (still known as the ICO), ref. ZC197792