

WHAT CAN AUSTRALIANS ACTUALLY GET REMOVED FROM SEARCH?

An evidence-based review of official privacy, online-safety and search-engine removal pathways in Australia

10

SCENARIOS

8

JURISDICTIONS

180

CODED FIELDS

178/180

DOCUMENTATION FIELDS
ASSESSED

Documentation coverage - not a removal success rate

SEARCH CLEANUP AUSTRALIA · ORIGINAL RESEARCH 2026

What Can Australians Actually Get Removed From Search?

An evidence-based review of official privacy, online-safety and search-engine removal pathways in Australia



10 SCENARIOS	8 JURISDICTIONS	180 CODED FIELDS	178/180 DOC FIELDS ASSESSED
------------------------------------	---------------------------------------	--	---

Research cut-off: 15 September 2026. This is a dated, qualified review of official documentation. It does not measure legal completeness, practical success rates or regulator effectiveness.

Publisher: Search Cleanup Australia · searchcleanupaustralia.com

Contents

2. Scope note
3. Funding and Conflict of Interest Disclosure
4. Executive Summary
5. Key Findings
6. Key Terms
7. What We Studied
8. What Australians Can and Cannot Request
9. Findings by Scenario
10. Federal Privacy / OAIC Pathways
11. eSafety Removal Pathways
12. Search-Engine Removal Pathways
13. State and Territory Comparison
14. Practical Removal Pathways
15. Source Removal vs Search De-indexing
16. News, Public Interest and Reputational Content
17. Methodology
18. Limitations
19. Data Availability
20. Selected Official Sources

2. Scope note

This study examines what official documents say a person can request, where the request goes, and what limits apply. It covers federal Australia, all six states, the Australian Capital Territory and the Northern Territory. Ten fixed scenarios range from exposed contact details to intimate-image abuse and unwanted news coverage. The national assessment contains 100 fields; the jurisdiction assessment contains 80.

The object being studied is a **documented pathway**, not the legal merits of an individual case. A request form establishes that someone can submit a request under stated conditions. It does not establish that a decision-maker must accept the request, that an investigation will follow, or that material will disappear. Similarly, an explanation of correction rights does not establish a right to delete a website.

Google and Microsoft documents are used as evidence of their own procedures and policies. Australian regulators and legislation are used for Australian regulatory and legal propositions. The review does not import European erasure rules into Australia. Its conclusions apply to the documents and versions inspected at the cut-off, with unresolved fields disclosed rather than filled by inference.

3. Funding and Conflict of Interest Disclosure

Search Cleanup Australia commissioned and publishes this study. It sells paid content-removal, search-cleanup, privacy and reputation-management services. That commercial interest could favour an expansive account of removal opportunities. The research design therefore requires narrow claims, official sources, explicit exceptions and an audit trail.

Readers can use the official pathways described here without hiring Search Cleanup Australia. No client outcomes, internal conversion data or internal commercial case results were used as evidence.

This is informational research, not legal advice. **This was an AI-assisted research and verification process, not independent human legal review.** Verification means that supporting official material was reopened and checked against its attribution. It does not mean that a human lawyer reviewed the interpretation or that an authority endorsed the study.

4. Executive Summary

Australians have documented routes to ask for personal information or harmful content to be corrected, removed, restricted or made less visible in search. The route depends on the information, who holds or publishes it, and the requested change. A publisher controls its page; a search engine controls its results; a platform applies its content rules; and a regulator acts within its jurisdiction. These functions do not amount to a universal power to erase a person's online history.

The final assessment contains **180 coded fields: 88 Yes, 87 Partially, 3 No clear guidance found and 2 Unknown / inaccessible. 178/180 fields were substantively assessed, or 98.89%**. This percentage measures how many of the fixed documentation questions could be assessed. It does not measure legal completeness, the proportion of real-world problems covered by a remedy, or the probability of removal. A Partially finding retains its conditions and limits; a No clear guidance found finding counts as an assessment, not as an available remedy.

The national matrix remains unchanged at **37 Yes, 60 Partially, 3 No clear guidance found and 0 Unknown**. The final jurisdiction matrix contains **51 Yes, 27 Partially, 0 No clear guidance found and 2 Unknown**. Only **ACT J03**, expressly documented individual deletion/erasure requests, and **ACT J07**, online publication/removal guidance, remain unresolved. Neither is a finding that the relevant right or guidance is absent.

The reviewed Australian framework does not establish a general EU-style Right to Be Forgotten. OAIC's comparative guidance distinguishes European erasure from Australian correction and conditional disposal duties. The reviewed current APP text and reform consultation preserve that distinction: proposed measures are not counted as operative rights. This conclusion does not decide whether another country's law could apply to a particular cross-border case. F11 F09 F10

The targeted recoveries sharpen the distinction between deletion and other changes. Victoria, Queensland and Tasmania expressly document deletion as a limited corrective action, with records and approval constraints. The Northern Territory finding concerns a particular agency's policy for information supplied to it. These findings do not establish general erasure rights. Context-specific publication and exposure guidance also exists for departmental images, public schools and planning submissions. R01 R03 R08 R13

Search policies can provide a route for specified personal information even where the information is true. Google identifies contact details, confidential identifiers and qualifying doxxing; Bing documents certain sensitive-information and intimate-image interventions. Their decisions concern their own results and remain subject to policy limits. They do not delete the original source. G01 B01

eSafety documents routes for serious adult abuse, child cyberbullying, image-based abuse and illegal or restricted content. Eligibility and reporting steps differ. Tasmania Police's explicit referral to eSafety supports threshold-limited findings, not a separate state power over private websites. ACT Education's referral remains a narrow school/family finding. E01 E02 E03 R09 R11

The report is suitable for publication as a **dated, qualified review of official documentation**. Its practical pathways can be used without buying a service. The two ACT gaps remain visible, and the evidence does not support jurisdiction rankings, estimates of legal effectiveness or claims about removal outcomes.

5. Key Findings

The final dataset answers most of the fixed documentation questions, while retaining important limits on what those answers mean. The assessment rate of **98.89%** is a statement about the dataset, not about the completeness or effectiveness of Australian law.

Finding	What it means for a reader
Source removal, search de-indexing and search-result refresh address different objects.	Identify the source page and each search result separately; record the scope of any response.
Express deletion findings are narrowly framed.	VIC/QLD/TAS corrective deletion is not general erasure; the NT finding is agency-specific.
Publication and exposure guidance can be context-specific.	Departmental image consent, public-school practice and planning-submission redaction cannot be generalised to every website.
eSafety referral is distinct from state regulatory power.	TAS findings depend on qualifying federal schemes; ACT referral evidence is limited to schools and families.
Statutory records can constrain destruction.	A record may need to be retained even where public access can be restricted.
ACT J03 and J07 remain Unknown / inaccessible.	Do not claim either the presence or absence of those routes from this study.
Submission and escalation do not establish an outcome.	An acknowledgement, investigation, policy approval and source change are different events.

The search/source distinction is explicit in the engines' documentation. The correction findings depend on express wording about deletion, rather than an inference from a general correction right or retention duty. The jurisdiction evidence and its scope notes explain the context-specific findings. G01 B01 R01 R03 R08 R13

Two examples illustrate why the requested action matters. NSW publishes a safety or wellbeing suppression process for specified registers, subject to a public-interest assessment. NT planning guidance allows an advance request to withhold identifying information from a published submission, while retaining the underlying record. Both concern public exposure; neither means that the holder destroys all information about the person. N04 R12

The practical starting point is to match the information, its holder, the desired change and the relevant rule. A refusal under one route does not decide whether a different route applies. Sections 9 and 14 explain that matching process for the ten frozen scenarios.

6. Key Terms

Term used in this report	Meaning
Source removal	The operator of the original page or service removes the material from that source.
Deletion or erasure	Information is removed from the record or system concerned; the scope must be checked, including any retained copies or statutory constraints.
Correction or amendment	A record is changed, supplemented or annotated to address a defect; the page or record may remain.
Suppression or restricted disclosure	Public access to specified information is limited while the holder may retain it.
Search de-indexing or delisting	A search engine removes a result within the scope of its decision. It does not thereby delete the host's copy.
Search-result refresh	A search engine updates its representation after the source disappears or materially changes.
Platform-policy removal	A service acts under its content rules; this is distinct from a finding under Australian law.
Regulatory escalation	A complaint is taken to an authority with relevant jurisdiction and procedural powers.
Court remedy	Relief available through a legal proceeding, subject to the cause of action, evidence, defences and procedure.

These are analytical labels used to keep the evidence intelligible. They are not presented as universally identical statutory definitions. In particular, the word “remove” in a support page must be read with its object: a result, image thumbnail, post, account, record or public-register entry.

“Personal information” also does not have one identical application across every document in this study. A search policy can enumerate particular identifiers while a privacy statute uses an identifiability test. A record can concern someone even when its contents are false. The applicable source must therefore be checked before treating ordinary language as a legal definition.

7. What We Studied

The ten scenarios were frozen before substantive research: residential-location exposure; phone or email exposure; identity, financial or sensitive-data exposure; inaccurate information; outdated information; doxxing; non-consensual intimate or sexual material; adult abuse or serious harassment; child bullying or harmful child content; and unwanted or damaging articles.

For every scenario, the national matrix asks about source removal, source correction, Google, another search engine, eSafety, privacy complaints, evidence, response or escalation, source/search distinction and limitations. Bing supplies the other-engine evidence. The research does not claim comprehensive coverage of every search product or individual hosting platform.

For each state and territory, the second matrix asks about oversight, correction, expressly documented deletion requests, complaints, public-sector scope, private-sector boundaries, publication guidance, exposure guidance, record limitations and federal referral. These are documentation criteria. The existence of an oversight body earns no assumption about its power over an unrelated overseas site.

The scenarios deliberately overlap. A threatening publication of an address may be both exposure and doxxing; a fake sexual image may be inaccurate information and image-based abuse. Cells are therefore not independent cases. Adding them produces a count of assessed questions, not a count of people, incidents, remedies or distinct entitlements.

The broad scenario wording also explains many Partial codes. A policy for particular identity numbers does not necessarily cover every type of sensitive information. An image policy does not cover all text involving a child. The frozen rule requires the broad field to retain that limitation instead of silently narrowing the scenario to the easiest category to document.

8. What Australians Can and Cannot Request

A person can ask a publisher to take material down, but a documented contact route is not necessarily an enforceable demand. The request becomes more precise when it identifies the information, the problem and the requested action: remove the address, correct the date, add the final outcome, restrict a register entry or remove a particular image result.

For covered records, Australian privacy documentation supports correction and complaints about mishandling. Disposal duties address when information should no longer be retained. Those duties contain conditions; they do not turn every objection to publication into an erasure right. Whether a holder needs information and whether it should expose that information publicly are separate questions. F06

Search-engine policy requests can be made without first establishing a court claim where the relevant policy applies. Conversely, the availability of a legal-reporting form does not prove that a legal claim exists. A person should not describe truthful content as unlawful merely because a legal option appears in a form's menu. G03

Desired result	Suitable question to put to the decision-maker
Correct a factual defect	What exact statement is wrong, and what evidence supports the proposed replacement?
Stop public exposure	Can the identified detail be removed, masked or withheld from this public page?
Remove a search result	Which policy or legal ground applies to this exact result and URL?
Update a stale search display	Has the live source actually disappeared or materially changed?
Escalate a privacy complaint	Is this holder and conduct within the authority's jurisdiction, and were earlier steps completed?
Obtain legal relief	Which cause of action and remedy fit the facts, and what defences or record rules apply?

Use these questions to prepare a request, alongside the requirements of the official form. It encourages a bounded request whose acceptance or refusal can be understood. "Remove everything about me" leaves the recipient to guess both the target and the claimed basis.

9. Findings by Scenario

9.1 Home address or residential location exposed online

A home address falls within Google's expressly listed personal-information categories. The broader term residential location could include material not exhaustively described by that list, so the composite Google field is Partial. A host request remains separate. A NSW licensing-register entry may instead warrant the specific suppression process in section 5. G01 N04

A useful request distinguishes the address from the surrounding story or record. If the aim is preventing contact at home, say which detail creates that exposure and which public copy contains it. Avoid assuming that removing an entire otherwise relevant document is the only possible outcome. The report makes no prediction about whether a narrower request will be accepted.

9.2 Phone number or personal email address exposed online

Google's documentation expressly lists both categories, producing a Yes for that search-policy field. Bing's examples expressly include private phone numbers and some confidential credentials, but are not an identical promise for every email-address case; the combined other-engine field remains Partial. G01 B01

Keep the distinction between a public contact listing and a compromised account. A removal request concerns what is displayed. Securing an account concerns continued access and misuse. This review does not measure the effect of either action on subsequent unwanted contact, so a disappearance from search should not be reported as proof that every copy or risk has gone.

9.3 Identity, financial or sensitive personal information exposed

Specified identifiers, financial details and private records appear in the engines' policies. "Sensitive information" is broader than any one enumerated list, which is why the composite route is Partial. A covered holder's security and retention duties may also be relevant, but do not automatically give a complainant control over all copies. G01 B01 F06

Describe the category accurately without unnecessarily repeating the full secret in correspondence. The official form's evidence instructions should govern what is supplied. Distinguish the entity that held the information from a third party that reposted it: the complaint against the holder and the request concerning the repost may concern different conduct and decision-makers.

9.4 Inaccurate personal information

The direct federal route is correction of qualifying personal information held by a covered entity. A request should identify the defect and proposed amendment. The Google legal channel is only a conditional alternative where a legal ground exists; it is not a general factual-arbitration service. False sexual association has a more specific policy route. F01 G03 G04

Separate a demonstrable error from an opinion or disputed interpretation. A document showing a different event date can support a precise amendment; disagreement with an author's evaluation requires a different explanation. This distinction helps keep the request evidentially clear without assuming that the study can decide a defamation dispute.

9.5 Outdated personal information

Outdated information can be a correction issue, but an old page and a stale search display are not the same problem. Google's refresh tool is for a source that has disappeared or significantly changed. It does not remove unchanged live material simply because the reader calls it outdated. Bing also identifies a tool for material already removed from the source. G02 B01

Compare the live page with the result before selecting a route. If they match, explain why the underlying record should change. If they differ, identify the removed or changed content. Record the date of that comparison; otherwise a later reviewer cannot tell whether the request concerned the current page or an earlier search representation.

9.6 Doxxing or malicious publication of personal information

Google describes qualifying doxxing in terms of personal data with threats or calls for harm, or substantial aggregation without a legitimate purpose. eSafety's adult-abuse material includes personal-detail exposure in severe abuse examples. The latter remains conditional on the applicable harm and Australian-connection requirements. G01 E04

Preserve context sufficient to distinguish exposure from a benign reference: associated messages, account details and the sequence of events can matter. This report does not determine whether a particular publication is a criminal offence. Its verified findings concern the search-policy route and relevant online-safety escalation, with detailed offence analysis left unresolved.

9.7 Intimate images or sexual material published without consent

eSafety documents direct reporting for qualifying image-based abuse, including certain fabricated or falsely attributed imagery. Google and Bing have relevant search policies. The scenario also includes wider sexual material, so the matrix does not generalise an image route to every sexual-text case. Consent and the Australian connection must be assessed under the chosen route. E03 G04 B01

Do not make contacting the person responsible a prerequisite. eSafety's blackmail guidance says to stop contact and not pay or provide further intimate material. Preserve permissible contextual evidence, but do not save or share sexual imagery of anyone under 18. Follow the official reporting instructions for that content. E03

9.8 Adult cyber abuse or serious online harassment

The adult scheme is reserved for severe abuse and has a high threshold. eSafety's procedure calls for reporting the content to the service first. A Google route in this matrix is conditional on an overlapping policy ground, such as doxxing; a general entitlement to delist every abusive comment is not inferred. E01 E04

Explain the target, context and nature of the harm, rather than supplying only an isolated insulting word. If a platform refuses, preserve the response and reference number. A refusal under one set of content rules does not decide whether a separate statutory threshold is met; equally, a report to eSafety does not guarantee intervention.

9.9 Child cyberbullying or harmful content involving a child

The child-bullying route concerns a person under 18 who ordinarily lives in Australia and content meeting the scheme's serious-harm definition. Other harmful child content may belong to the illegal/restricted-content or intimate-image track. Google's minor-image policy applies to qualifying image URLs, not every webpage discussing a child. E01 G05

The adult helping with a report should establish their authority and use the correct content category. Keep records of earlier platform reports. The evidence rule is especially important here: an instruction to preserve evidence is not an instruction to download illegal imagery. URLs and contextual reporting information should be handled through the official process. E02

9.10 Old, unwanted or reputationally damaging news or articles

The reason for objection determines the possible route. A factual error, private identifier, qualifying abuse, stale result and alleged legal wrong are different issues. Mere age or reputational discomfort is not identified as a standalone Australian removal entitlement. Journalism coverage and public-interest policy limits are material. F04 G03

List the requested change separately from the overall complaint. A request to add a later outcome is different from a demand to erase accurate historical reporting. If legal action is contemplated, the issue requires case-specific advice; this study did not verify a complete defamation or court-record pathway and does not supply one by analogy.

10. Federal Privacy / OAIC Pathways

The first federal question is whether the relevant holder and conduct are covered. OAIC explains coverage for Commonwealth agencies and relevant organisations, alongside exclusions. Many small businesses fall outside the general framework, but specified exceptions can apply, including health-service and certain information-trading activities. A small-business label alone is therefore insufficient to decide jurisdiction. Journalism, employee records and personal-capacity activity also require attention. F04 F05

Do not assume that residence in Australia makes every online publisher an APP entity. Nor should the geographical location of a server replace assessment of the entity and conduct. The practical starting point is to identify who collected, held, disclosed or published the information and why that person's conduct is said to fall under the framework.

For correction, the current Act distinguishes agency timing from organisation timing: APP 13 specifies 30 days for agencies and a reasonable period for organisations. OAIC's consumer guidance treats 30 days as a reasonable correction period. The legislation also addresses written refusal, associated statements and notification to another APP entity after correction, subject to its conditions. These are procedural rights, not a promise that the requested replacement wording will be adopted. F09 F01

For complaints, OAIC tells individuals to raise the matter with the entity first. A complaint can follow an unsatisfactory response or no response within 30 days, with an approved external dispute-resolution scheme sometimes being the appropriate preceding route. The complaint should identify the entity, events, earlier correspondence and outcome sought. Representation requires the appropriate authority. F02

OAIC is an impartial decision-maker, not the complainant's advocate. It may decline matters outside coverage or where procedural conditions are unmet. Assessment, conciliation and a possible determination are different stages. A request for a particular outcome does not require the authority to provide it, and a penalty against an entity is not automatically compensation to the complainant. F03

A separate development is the statutory tort for serious invasions of privacy, which commenced on 10 June 2025. It is administered through courts, not OAIC's complaint process. The reviewed statutory elements include intentional or reckless serious invasion, reasonable expectation of privacy and the public-interest balance. OAIC identifies possible injunctions, damages and apologies, alongside defences and exemptions. This route must not be reduced to "ask OAIC to remove it". F09 F07

This report identifies the court route without providing a litigation checklist. Whether proceedings are appropriate depends on facts, relief, limitation rules and potential defences. The existence of a court remedy is relevant to the map of pathways; it does not make legal proceedings interchangeable with submitting a free regulator form.

The Attorney-General's 2026 consultation is treated as a temporal boundary. It opened on 31 August and closes on 18 September 2026, and its page says the bill remains subject to government consideration. No proposed entitlement is coded as an operative right. That is the status recorded at the research cut-off; this report does not predict subsequent reform. F10

11. eSafety Removal Pathways

The eSafety routes are organised around harmful content and statutory thresholds. They are not general-purpose correction or reputation services. A person selecting a route needs to consider age, Australian connection, content type, seriousness and previous reporting. A report that fails one track may describe something materially different that belongs in another; that possibility must be assessed from the facts.

For adult abuse and child cyberbullying, the verified instructions require an earlier report to the relevant platform or service. For qualifying image-based abuse, the person can report directly to eSafety. The reporting guidance also distinguishes illegal and restricted content and provides specialised instructions for sexual extortion. These steps should not be collapsed into one universal sequence. E01 E02 E03

eSafety explains that it can, in qualifying cases, direct services to remove content and take further action over noncompliance. A notice is an exercise of statutory powers in a particular case. It is not a blanket statement that every reported item will receive a notice, or that all copies on unrelated services will disappear. E02

The evidence should allow the investigator to locate and understand the content. A practical record can include URLs, profile identifiers, dates and previous report references. Screenshots are not appropriate for illegal imagery. In particular, do not save or share sexual images or videos of anyone under 18; follow the official instructions instead. The study makes no recommendation to collect such material independently. E02 E03

Keep two questions separate when reading a response: did the report provide enough information for assessment, and did the content meet the scheme? Additional detail may address the first without changing the second. Neither an acknowledgement nor a request for more evidence is a finding that the statutory threshold has been satisfied.

The three national “No clear guidance found” cells concern a standalone eSafety route for mere inaccuracy, age of information or unwanted reputation. Scheme checklists and reporting instructions were successfully reviewed for those questions. The finding does not exclude eSafety where the same article also contains qualifying abuse or intimate imagery. It records the absence of a distinct route for the bare scenario, not an absolute legal conclusion.

12. Search-Engine Removal Pathways

Search policies and legal requests should be read separately. A platform may voluntarily adopt a policy covering specified personal data. A legal request asks it to consider a legal basis. The evidence for one does not establish the other, and neither automatically changes the original website.

Google's personal-information process specifies URLs and explains that its decision may remove a result generally or only for searches containing a name or identifier. Public interest can affect its decision. The meaning of an approval therefore depends on its actual scope. A reader should not report an entire website as erased when the decision concerns one result or one class of queries. G01

Google's sexual-content and minor-image policies are distinct from that general process. Their qualifying categories, representation rules and eligible URL types matter. In particular, the non-explicit minor-image policy specifies image URLs and excludes the whole text-and-image webpage from that particular removal route. G04 G05

The refresh tool serves another purpose. It is designed for removed or significantly changed source material. It requires a Google account, identifies the requested URL and supplies status information, including reasons for denied requests. Refreshing a changed page can remove the old snippet while leaving a result that is later updated. G02

Bing documents certain sensitive-information and intimate-image removals, legal-demand assessment and a stale-content route. Its page links to the relevant reporting tools. The study does not infer an Australia-wide erasure entitlement from its references to removal laws in other countries. Its explanation of how search results are ordered does not establish a right to a preferred position in those results. B01

For legal reports to Google, select the relevant product, supply exact URLs, identify the contested content and explain the legal basis. The page provides confirmation and follow-up procedures. Separate products require separate notices. A legal-report form is an intake route; the underlying legal claim must still be justified. G03

A useful personal request log has a row for each engine, URL, submission date, reference, stated ground and response. That is an organisational suggestion from this report. It helps prevent a decision about one engine being mistaken for a decision about another, without assuming that repeated submissions improve the outcome.

13. State and Territory Comparison

The comparison follows the frozen jurisdiction order. It does not rank jurisdictions. Public-sector correction and complaint routes may include specified health or contractor activities, but an oversight body is not assumed to regulate every private website viewed by residents. The final jurisdiction matrix contains **80 fields: 51 Yes, 27 Partially, 0 No clear guidance found and 2 Unknown / inaccessible**.

Reading the recovered findings

The table reproduces the final codes for the criteria central to the recovery pass. **J03** asks whether an individual deletion/erasure request is expressly documented; **J07** concerns online publication/removal guidance; **J08** concerns doxxing/personal-information exposure guidance; **J09** concerns court/public-record or statutory-record limitations; and **J10** concerns a clear federal regulator/eSafety referral where applicable. “Unknown” below is the exact dataset category **Unknown / inaccessible**, shortened for readability. Partially always retains the limitations explained after the table.

Jurisdiction	J03	J07	J08	J09	J10
New South Wales	Partially	Partially	Partially	Yes	Yes
Victoria	Partially	Partially	Partially	Partially	Yes
Queensland	Partially	Partially	Partially	Yes	Yes
Western Australia	Partially	Partially	Partially	Yes	Yes
South Australia	Partially	Partially	Partially	Yes	Yes
Tasmania	Partially	Partially	Partially	Yes	Yes
Australian Capital Territory	Unknown	Unknown	Partially	Yes	Partially
Northern Territory	Partially	Partially	Partially	Yes	Yes

A Yes for J09 means that a relevant limitation is documented, not that deletion is available. J08 can be supported by narrow personal-information exposure guidance without a comprehensive doxxing procedure. J10 records a referral, not a transfer of federal powers to a state authority. The full ten-criterion matrix is in `jurisdiction_coding_final.csv`.

13.1 New South Wales

The IPC describes public-sector and health-information coverage, amendment and complaint routes. Appropriate deletion can form part of correction; the erasure criterion remains Partially. The register-suppression process concerns specified NSW Fair Trading and Building Commission registers and requires consideration of public interest. It restricts public disclosure rather than destroying the underlying licensing record. N01 N02 N03 N04

13.2 Victoria

OVIC distinguishes FOI amendment from Privacy and Data Protection Act correction for relevant organisations outside the FOI route. It explains public-sector coverage, separate health oversight and federal referral; complaints begin with the organisation. V01 V02

J03 is Partially. OVIC's section 49 guidance expressly permits corrective deletion or expungement, and exceptionally destruction, with the Keeper of Public Records' agreement. It requires consideration of the request and records constraints. This is an express but limited form of correction, not a general right to erase accurate or unwanted information. R01

J07 and J08 are Partially. OVIC's breach guidance describes removing an inadvertently leaked online document and assesses exposure risks involving a victim's name and address. It provides agency breach-response guidance, not a universal individual takedown process. The existing J09 Partially code remains unchanged; the report does not turn these examples into a complete court-record suppression procedure. R02

13.3 Queensland

OIC's public guidance explains the Queensland Privacy Principles, private-sector boundaries and federal referral. The existing correction criterion remains Partially. Its complaint process allows the agency 45 business days before OIC escalation may be available; mediation and possible tribunal referral are distinct stages. Q01 Q02

J03 is Partially. OIC's amendment-decision guidance expressly includes deleting incorrect factual information as a form of alteration. It excludes destruction or disposal of the entire document, and preservation requirements may make notation appropriate instead. The recovery does not create a general erasure right. R03

J07 is Partially because Justice's consent terms provide for a private message requesting removal of consented images or recordings when consent is revoked. This concerns the department's own promotional use, not every publisher or retained copy. **J08 is Partially** because OIC explains agency data breaches, serious harm, notification and protective advice. This is a scoped exposure finding, not a general doxxing-removal power. R04 R05

13.4 Western Australia

OIC's newer complaint guidance covers alleged interferences from 1 July 2026. It separates government-document FOI correction from the relevant contractor privacy route. Legal Aid WA's FOI guidance expressly includes corrective deletion; the existing J03 code remains Partially. Older contextual wording is not used to expand the proposition. W01 W02 W03 W04 W05

J07 and J08 are Partially. Public-school procedures require permission and privacy clearance for internet publication of student images and work, limit identifying details, and address inappropriate school-page content. They also cover exposure of names, addresses, photographs and contact details. These are public-school publication and protective practices. Hiding or blocking a post is not destruction of its source or search de-indexing, and the procedures are not a jurisdiction-wide takedown route. R06

13.5 South Australia

State Records explains the agency scope of the Information Privacy Principles Instruction. Councils and universities are not simply folded into that mandatory scope. The Privacy Committee's complaint and recommendation role is distinct from an automatic deletion order. Photograph guidance addresses internet publication and removal where possible; the existing deletion/publication findings remain narrow. S01 S02 S03

J09 is Yes. State Records expressly explains statutory disposal controls, permanent archival retention and prescribed retention periods for temporary records. This verifies a records limitation. It does not establish an individual deletion right or a universal rule for removing court records. R07

13.6 Tasmania

The Ombudsman identifies covered custodians and an entity-first complaint process. Correction and complaint time limits remain subject to the qualifications in that guidance. T01 T02

J03 is Partially. The recovered whole-Act text allows a person to request specified amendments. Section 17I expressly addresses corrective deletion, expungement and destruction, requiring State Archivist agreement. The request must concern incomplete, incorrect, outdated or misleading information; this is not general erasure. **J09 is Yes** because section 17I and Schedule 1 clause 4(3) document Archivist controls on relevant destructive correction and disposal. A disposal duty is not an individual deletion entitlement. R08

J07 and J08 are Partially; J10 is Yes. Tasmania Police explicitly adopts a reporting pathway to eSafety, describes removal of qualifying harmful content, and includes doxxing within its adult-abuse explanation. The state authority's express referral supports J10. The publication/removal and exposure findings remain conditional on the federal schemes and their thresholds. They do not establish a separate state privacy power over every private website. Reporting steps should be read with the verified national eSafety guidance in section 11; the state page is not used to impose a universal waiting period. R09

13.7 Australian Capital Territory

The Human Rights Commission's guidance covers ACT public-sector bodies and certain contractors, complaint requirements and conciliation. It also describes a possible Magistrates Court application after specified findings and an unresolved complaint. The existing correction and private-sector-boundary codes remain Partially; the TPP summary is not a complete request guide. A01 A02

J08 and J10 are Partially. Access Canberra documents identity-exposure responses, including replacement of a compromised licence card and account-protection steps. That supports a narrow exposure finding, not a doxxing or website-erasure right. ACT Education adopts eSafety recommendations and refers parents and students to cyberbullying and image-abuse resources. This is a school/family referral, not a comprehensive adult or private-sector referral map. R10 R11

J03 and J07 remain Unknown / inaccessible. Accessible correction and retention material did not establish an express deletion procedure, while relevant Digital Account and school-manual leads could not be substantively reviewed. The available material was insufficient for a positive finding or a defensible No clear guidance found assessment. The eSafety referral does not fill the separate online publication/removal gap. The unresolved-fields record preserves the retrieval reasons; neither cell establishes that a right or guidance is absent.

13.8 Northern Territory

The Information Commissioner documents written correction requests to the holder and statements associated with disputed records. Its guidance limits historical-only information and explains complaint prerequisites and relevant federal referrals. D01 D02

J03 is Partially. Tourism and Events NT expressly accepts written requests to delete personal information provided by the requester, considers them individually and gives a written response. This agency-specific policy does not establish a Territory-wide entitlement or guaranteed approval. R13

J07 and J08 are Partially. DLPE explains planning-submission publication and allows an advance request to withhold identifying details. A granted request affects the published submission, while the underlying record is retained and remains subject to statutory controls. This is context-specific protection against exposure, not a general doxxing or internet-removal procedure. R12

14. Practical Removal Pathways

Use the following table with the corresponding scenario in section 9 and the official links in sections 10–13 and 20. Read the linked official source before submitting, because categories and forms can change. Each path is available without purchasing a Search Cleanup Australia service. “Privacy route” means a complaint about covered information handling, not a guaranteed order to delete.

Scenario	First contact and evidence	Search / regulator route	If refused; main limit
Home address	Host or responsible public-register agency; exact URL and exposure context.	Google personal information; privacy complaint if covered; eSafety if serious abuse.	Read the reason, check scope and use the applicable complaint route. Search action leaves the host copy.
Phone or email	Host/service; identify the contact detail and page.	Google policy; Bing where its specified risks apply; conditional privacy or eSafety route.	Preserve reference and response. Not every public business contact is equivalent to private exposure.
Identity/financial/sensitive data	Holder and hosting service; identify the data category with permissible evidence.	Relevant engine policy; covered-entity privacy complaint; eSafety only with qualifying harm.	Explain the exact policy or handling issue. Broad sensitivity alone does not satisfy every policy.
Inaccurate information	Holder/publisher; disputed statement, proposed correction and supporting record.	Correction/privacy route; conditional engine legal or specific false-sexual-content route.	Ask for written reasons and applicable statement/complaint options. Correction is not whole-page deletion.
Outdated information	Compare source and result; ask holder to update defective current information.	Refresh after source change; conditional correction complaint.	If unchanged, reassess the source issue. Age alone is not a refresh ground.
Doxxing	Platform; URLs, threats, aggregation and context.	Google doxxing; eSafety for qualifying serious abuse; privacy if covered.	Preserve earlier report; escalate under the correct scheme. Not every mention of a person meets its threshold.
Intimate material	Direct eSafety reporting is available for eligible imagery; use safe contextual evidence.	Separate Google/Bing search requests; other privacy route only if covered.	Follow eSafety support and assessment guidance. Do not contact or pay a blackmailer; do not save child sexual imagery.
Adult abuse	Platform first; account identifiers, dates, context and report reference.	eSafety if threshold met; engine route only where a separate policy/legal ground applies.	Submit the platform response with escalation. Serious-harm criteria restrict the scheme.
Child harm	Appropriate platform and reporting track; establish age and representative authority.	Child-bullying, image-based or illegal-content route; eligible Google image route separately.	Follow safe evidence rules and preserve earlier reports. One child-image policy does not cover all text.

Scenario	First contact and evidence	Search / regulator route	If refused; main limit
Unwanted news	Publisher; identify error, exposed detail or requested contextual update.	Conditional privacy, search-policy or legally based request; refresh only after source change.	Seek reasons and case-specific advice for legal allegations. Reputation alone supplies no documented entitlement.

The accompanying `practical_pathways.csv` separates each requested question: first contact, evidence, source, Google, eSafety, privacy, refusal, escalation and limitation. It also supplies official URLs. Its practical ordering is an editorial synthesis of verified sources, not a tested procedure or an outcome guarantee. Where Bing is relevant, the file includes its separate pathway rather than implying a Google decision applies across engines.

Before submitting, prepare a short factual chronology. Distinguish what you observed from what you infer. Record when the content was found, what it displayed, the exact requested action, and any response. If a new copy appears, record it as another copy rather than overwriting the history of the first.

Do not treat this chronology as a reason to preserve prohibited material. The safe-evidence instructions in sections 9 and 11 prevail. Where immediate danger is present, eSafety directs people in Australia to emergency services on 000; an ordinary search-removal request is not an emergency response. E02

After any approval, describe only the confirmed action. A host's confirmation, a corrected page and a search notification are different evidence. The report recommends recording those outcomes separately to avoid an ambiguous statement such as "the internet has been cleaned". This is a documentation practice, not a claim that monitoring produces a particular result.

15. Source Removal vs Search De-indexing

A page can remain available by its direct address after a search engine removes a link. It can also remain accessible through another engine, a social link or a copy elsewhere. Google's and Bing's documentation expressly distinguishes their results from hosting. G01 B01

The reverse situation matters too. A publisher can change a page while an engine still displays an earlier representation. A refresh request concerns that mismatch. It is not proof that the publisher failed to act, and a refresh refusal may mean the live-source conditions for the tool were not met. G02

Observed situation	What can accurately be said	What remains to be checked
Publisher confirms address redaction	The publisher reports removing that detail from the identified page.	Whether the live page reflects it and whether separate copies remain.
Search approval identifies a URL	That engine approved the specified result action.	Scope, query restrictions and other engines or sources.
Search result now reflects a correction	The inspected result displayed the updated information at that time.	Other results and whether any retained record has a separate purpose.
Regulator acknowledges complaint	The complaint was received.	Jurisdiction, acceptance, investigation and outcome.
Court relief is available in principle	An official source documents a potential legal remedy.	Whether the individual facts satisfy the requirements and relief is granted.

This distinction also improves reporting about the study itself. A dataset row coded Yes means the relevant documentation exists. It does not mean that a hypothetical applicant obtained any of the outcomes in the table. There were no test submissions and no observed client cases in this research.

16. News, Public Interest and Reputational Content

The old-news scenario is especially susceptible to overstatement. “This harms my reputation” describes an impact, but does not by itself identify a correction ground, a policy category or a legal wrong. The request needs to specify what makes the publication actionable under the chosen route.

A false factual statement differs from accurate historical reporting. A later development may justify asking for an update, but the study does not infer a duty to rewrite history. Personal information inside an article can raise a distinct issue from the article as a whole. Likewise, a search result can be stale even when the underlying reporting has already been corrected.

Public interest is not just a publisher's slogan in the reviewed material. Google identifies newsworthiness as relevant to its personal-information decisions. Federal privacy coverage includes a journalism exemption with specified conditions. The statutory privacy tort also requires attention to countervailing public interests and exemptions. These are separate legal and policy tests, not one interchangeable exception. G01 F04 F07

Alleged defamation requires its own analysis. OAIC's online-safety guidance refers people with defamatory-material concerns to legal help. This review did not obtain sufficient verified substantive material for a comprehensive defamation procedure or state-by-state limitation account. It therefore identifies that possible legal issue without declaring content defamatory or promising a removal order. F08

Court judgments, statutory registers and other official records require particular care. The NSW suppression example, SA and TAS retention controls, and NT planning-record guidance show why a general correction summary cannot resolve every public-record question. N04 R07 R08 R12 This report does not claim that Google approval binds a court registry, or that a corrected private webpage changes an official record.

An accurate public-facing description is consequently conditional: a reader may have a publisher request, a correction issue, a qualifying search-policy ground or a legal claim, depending on the content and context. There is no evidenced general entitlement to remove an accurate article solely because it is old, unwanted or commercially inconvenient.

17. Methodology

The protocol was frozen before substantive research. It fixes the scope, ten scenarios, national and jurisdiction criteria, coding definitions, source hierarchy and verification rules. Its recorded digest is preserved in the integrity documentation. No scenario, criterion or denominator was changed to improve the assessed percentage.

The design contains a ten-scenario by ten-criterion national matrix and an eight-jurisdiction by ten-criterion matrix: **100 national fields and 80 jurisdiction fields, 180 in total**. The jurisdiction criteria concern the relevant public-sector regime, with private-sector and federal boundaries recorded explicitly. Overlap between scenarios is intentional; cells are not independent people, cases or legal entitlements.

Research used Australian-English official-domain searches, direct navigation, FAQs, guidance, forms, decisions where relevant, and linked legislation or PDFs. Search snippets were used for discovery only. The primary federal legal compilation was recovered through the official download view. During the final targeted pass, the Tasmanian Act's whole-document view supplied text that earlier extraction had not exposed. Retrieval failure was never treated as proof that a remedy was absent.

Supporting sources were reopened in a separate verification pass to check official identity, resolution, actual text and scope. Each positive cell has a scoped evidence record. Verification did not treat a party's submission as an authority's reasoning, platform policy as legislation, or search delisting as source deletion. Only VERIFIED evidence supports Yes or Partially findings.

The final targeted recovery was confined to the previously unresolved jurisdiction fields. It recovered 19 of 21: **3 Yes and 16 Partially**, with **0 conversions to No clear guidance found** and **2 remaining Unknown / inaccessible**. Every positive recovery was separately reopened and checked before application. National coding and all non-target jurisdiction cells stayed unchanged. The change ledger identifies the cells and supporting sources.

Code	Frozen meaning
Yes	Direct and sufficiently clear official evidence supports the criterion.
Partially	Official evidence addresses the issue narrowly, indirectly, conditionally or incompletely.
No clear guidance found	Successful access and a reasonable official-source search did not reveal clear guidance on that specific point.
Unknown / inaccessible	Retrieval, extraction or substantive evidence was insufficient to assess the field.

A positive code does not imply a successful outcome. A negative search assessment is not proof that no legal route exists. Unknown remains distinct from both. These definitions are unchanged from `research_protocol_v1.md`.

Final code	National	Jurisdiction	Overall
Yes	37	51	88
Partially	60	27	87

Final code	National	Jurisdiction	Overall
No clear guidance found	3	0	3
Unknown / inaccessible	0	2	2
Total	100	80	180

Substantively assessed coverage is $(88 + 87 + 3) / 180 \times 100 = 98.89\%$, rounded to two decimal places: **178/180 fields**. The numerator includes No clear guidance found because it is an assessment; the denominator retains Unknown. This is the approved documentation-coverage calculation, not a removal rate or measure of legal completeness.

Initial research and verification took place on 14 September 2026, with the targeted recovery and final dataset cut-off on **15 September 2026**. Access dates record the actual session in which material was inspected. Visible source dates, commencement dates and missing dates remain separately identified. The editorial pass reconciled the report with this final dataset; it did not conduct new research, change coding or reopen the methodology.

The source set is not a random sample of disputes. Some cells rely on the same document. There is no sampling basis for estimating removal probability, comparing regulator effectiveness or calculating confidence intervals for case outcomes. Practical request ordering is editorial synthesis, not evidence from test submissions.

18. Limitations

98.89% assessed does not mean 98.89% legally complete or practically covered. It means that 178 of the 180 frozen documentation questions received an assessment other than Unknown / inaccessible. Narrow and conditional Partially findings remain narrow and conditional. The three national No clear guidance found cells contribute to assessment coverage but do not identify available remedies.

Two fields remain unresolved:

Jurisdiction and field	Evidence gap	Consequence for interpretation
ACT J03 — Individual can request deletion/erasure where expressly documented	Accessible correction/retention material did not establish the remedy; relevant procedural retrieval remained insufficient.	The study cannot conclude either that an individual deletion route exists or that none exists in the ACT.
ACT J07 — Online publication/removal guidance found	Relevant procedural/manual material could not be substantively retrieved. General privacy statements and eSafety referrals do not resolve the field.	Keep ACT publication/removal documentation unresolved; do not substitute a referral for a source-removal right.

These gaps materially limit complete all-jurisdiction claims about deletion requests and online publication/removal. They do not invalidate the separately verified routes. The remaining_unknowns_final.md and verification log explain the access problems; neither Unknown cell is treated as No clear guidance found.

Coverage limits also remain within assessed fields. Corrective deletion, an agency-specific policy, public-school guidance, departmental image consent and planning-submission redaction cannot be described as universal rights. A statutory records constraint documents a limit on destruction, not a deletion entitlement. A state authority's referral to eSafety establishes neither a separate state removal power nor eligibility under every federal scheme.

Detailed defamation remedies, criminal doxxing provisions, court-record suppression procedures and all state-law retention exceptions were not comprehensively verified. The record-limitation findings do not supply a complete court-remedy guide. An omitted route must not be described as unavailable solely because it falls outside the verified material.

Some official material retains older or broader wording. The research uses it only for the propositions checked and scoped in the evidence table. Historic OAIC comparative guidance is read with the reviewed APP text and reform status. Older contextual wording in Legal Aid WA is not used for ACT referrals. Tasmania Police's referral page is not used to impose a universal 48-hour reporting rule, and Access Canberra's broad notification summary is not used to assert a universal legal notification duty. The national pathways remain as verified in the frozen dataset.

No request form was submitted, complaint lodged or individual case tested. The study did not measure administrative delay, practical accessibility, translation quality, emotional burden, legal expense or enforcement outcomes. Stated timeframes are cited procedural requirements or guidance, not measured average removal times.

The same AI-assisted process carried out research and verification. A separate reopen checks attribution; it is not independent replication, independent human legal review or an authority's endorsement. Links are supplied for readers to consult official material, but the report records a dated research state and does not guarantee that every page or procedure will remain unchanged.

The report is publication-ready **as a qualified documentation review with these limitations retained**. It is not a comprehensive legal opinion, a jurisdiction comparison by effectiveness or a promise of practical results.

19. Data Availability

The accompanying research files allow the report's coding and attributions to be inspected without specialist software or a paid service. The frozen final research state consists of the following files; this report does not replace or modify them.

Purpose	Authoritative file(s)
Frozen design and definitions	research_protocol_v1.md
National matrix — unchanged	national_scenario_coding.csv
Final jurisdiction matrix	jurisdiction_coding_final.csv
Scoped positive evidence	evidence_table_final.csv
Sources and their status	source_register_final.csv
Source reopening, attribution checks and unsuccessful attempts	verification_log_final.csv
Ten practical scenario pathways	practical_pathways.csv
Targeted recovery decisions	targeted_recovery_21.csv
Final dataset checks and unresolved fields	integrity_report_final.md; remaining_unknowns_final.md

The CSVs use UTF-8 encoding and descriptive headers. National rows have stable N01–N10 identifiers; jurisdiction rows use NSW, VIC, QLD, WA, SA, TAS, ACT and NT. National criteria are C01–C10 and jurisdiction criteria J01–J10. Evidence records connect individual cells to source IDs, official URLs, sections, paraphrases, scope limits and verification entries. Bracketed source IDs in the report link directly to official pages; section 20 supplies their titles. The source register supplies the precise sections and scope notes.

The final evidence table contains **175 VERIFIED positive-cell records**, including the 19 verified recovery records. Records are not independent sources or observed cases. Multiple cells can cite one official document. The source and verification registers also retain unsuccessful or superseded recovery attempts; entries marked UNVERIFIED are not positive evidence.

The original Draft_Report.md and baseline research files are preserved. Final_Report_2026-09-15.md is the reconciled publication version. Publication_Notes_Final.md describes editorial treatment, while Final_Editorial_Integrity_Audit.md records the checks against the authoritative final files. No new coding or metrics beyond the approved dataset totals were introduced in the editorial pass.

Research dates and source publication/update dates remain distinct. Any later research update should be separately dated and identify changed sources and cells. The present report must continue to be described by its 15 September 2026 cut-off.

20. Selected Official Sources

The following register keys identify the principal official source families. Full titles, URLs, access dates, sections and verification status are provided in `source_register_final.csv`. The live links below also allow direct review of the principal procedures.

Topic	Official sources
Federal correction and complaints	F01 — Correct your personal information; F02 — Before you lodge a privacy complaint with us; F03 — How we investigate and resolve your complaint
Federal scope and security	F04 — Rights and responsibilities; F05 — Small business; F06 — Chapter 11: APP 11 — Security of personal information
Current Act and serious privacy invasions	F09 — Privacy Act 1988, compilation 104; F07 — Statutory tort for serious invasions of privacy
Erasure comparison and current reform status	F11 — Australian entities and the European Union General Data Protection Regulation; F10 — Privacy Reform – Consultation on Exposure Draft legislation
Google information, refresh and legal reporting	G01 — Remove my private info from Google Search; G02 — Refresh Outdated Content tool; G03 — Report content for legal reasons
Google sexual content and minor images	G04 — Remove personal sexual content from Google Search; G05 — Remove images of minors from Google search results
Bing policy and reporting links	B01 — How Bing delivers search results
eSafety eligibility and reporting	E01 — What you can report to eSafety; E02 — How to report serious online abuse, illegal and restricted content; E03 — Report image-based abuse; E04 — Adult cyber abuse
New South Wales	N01 — Privacy; N02 — Request personal information; N03 — Make a complaint; N04 — Request to have personal information suppressed
Victoria	V01 — Your privacy rights; V02 — Privacy complaints
Queensland	Q01 — Queensland privacy rights; Q02 — How to make a privacy complaint
Western Australia	W01 — Understanding my privacy rights: when do they commence?; W02 — What are my privacy rights? A resource for the public; W03 — How to make a privacy complaint; W04 — Information Privacy Principles Summary; W05 — Privacy and freedom of information
South Australia	S01 — Making a privacy complaint; S02 — Information for the public; S03 — Photographs and privacy
Tasmania	T01 — Personal Information Protection; T02 — Ten Personal Information Protection Principles
Australian Capital Territory	A01 — Complaints about breaches of privacy; A02 — Territory Privacy Principles quick reference
Northern Territory	D01 — Correcting information: overview; D02 — Make an inquiry or complaint

Verified targeted-recovery sources

These additional sources support only the scoped recoveries described in section 13. Alternative pages and failed attempts in the source register are not promoted to positive evidence.

Jurisdiction / subject	Verified official sources
Victoria — corrective deletion and breach response	R01 — Section 49 R02 — Managing the privacy impacts of a data breach
Queensland — amendment, departmental images and exposure	R03 — Decision making - amendment applications R04 — Consent for use of images through social media R05 — What is Queensland's data breach scheme
Western Australia — public-school online practice	R06 — Students Online in Public Schools Procedures
South Australia — statutory disposal controls	R07 — Disposal and Disposal Schedules
Tasmania — corrective deletion, records and police referral	R08 — Personal Information Protection Act 2004 R09 — Dealing with online abuse
ACT — identity protection and education referral	R10 — Protect your identity after a data breach or cyber-attack R11 — Online safety and security
Northern Territory — planning publication and agency deletion policy	R12 — Privacy of planning submissions R13 — Privacy policy

Final dataset: 180 coded fields; 88 Yes; 87 Partially; 3 No clear guidance found; 2 Unknown / inaccessible. Substantively assessed: 178/180, or 98.89%. The unresolved fields are ACT J03 and ACT J07.