Unlock
for people with criminal records

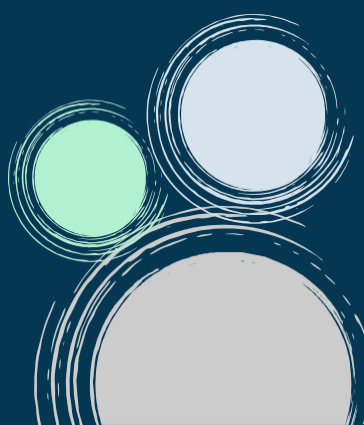
The Right to be Forgotten

Unlock Briefing
December 2025

Google - you know my name but don’t judge me until you know my story.

About Unlock

Unlock is a national independent advocacy charity that supports, speaks up and campaigns for people facing stigma, prejudice and discrimination because of their criminal record. We work in England and Wales.

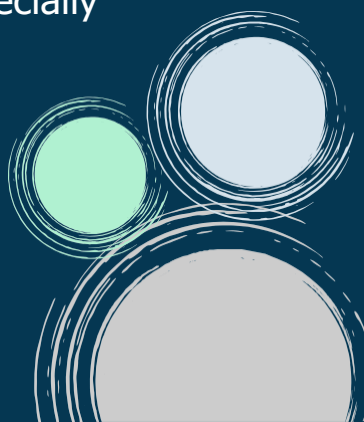


Executive summary

This briefing examines how the digital age has undermined the promise of the Rehabilitation of Offenders Act 1974 (ROA) and sets out reforms needed to protect the right to move on from a criminal record.
The ROA was designed for an analogue world in which criminal record information was accessed only through formal channels and with the individual's knowledge and consent. Today, online news archives, search engines, social media and rogue "naming and shaming" sites mean that criminal records – including spent convictions – can remain searchable indefinitely. Employers, education providers and others can easily discover information online that they would not lawfully receive via a Disclosure and Barring Service (DBS) check.

The report explains the DBS framework (basic, standard and enhanced checks) and shows that, in principle, how this system ought to balance safeguarding with rehabilitation. In practice, however, the availability of online information bypasses DBS safeguards, giving employers uncontrolled access to partial and often inaccurate criminal record data. Many routinely conduct online searches – including via search engines, social media and AI tools – without a lawful basis or clear policy on how to handle any criminal record information they find. This creates serious risks of unlawful data processing under UK GDPR and systemic discrimination.

The harms are unevenly distributed. People with non-anglicised names are more easily searchable, compounding existing racialised discrimination in recruitment. Women are more likely to attract sensationalist media coverage, often linked to trauma and poverty, and are at particular risk from abusive ex-partners who can track them online. Families, especially children, may suffer stigma and bullying linked to a parent's digital footprint.



Living under this "long shadow" of a criminal record contributes to anxiety, depression, social withdrawal, loss of employment and housing opportunities, and can undermine desistance and trust in state institutions.

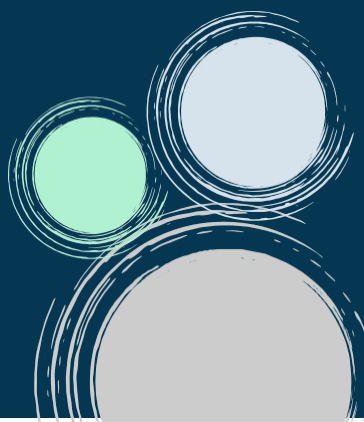
This briefing situates these harms within the broader legal landscape of the 'right to be forgotten'. It explains how delisting from search results – grounded in GDPR and shaped by cases such as Google Spain and NT1 & NT2 v Google – offers a potential remedy but is in practice complex, inconsistent and opaque. Delisting is not automatic when a conviction becomes spent, criteria for "public interest" are unclear, and decisions by tech companies lack transparency. Even when delisting is granted, articles remain at source, and partial delisting can still leave individuals exposed.

Regulatory mechanisms are fragmented and underpowered. The Information Commissioner's Office (ICO) can act where criminal record data is inaccurate, unlawfully processed or retained for longer than necessary, including in relation to vigilante sites. However, cross-border hosting, volume of content and procedural delays limits the ICO's impact. The Independent Press Standards Organisation (IPSO) Editors' Code offers safeguards against misleading, outdated and prejudicial reporting, but these can be ignored in criminal justice coverage, and individuals frequently lack awareness of complaint routes.

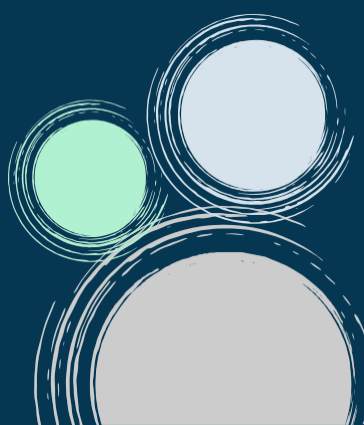
Recent policy developments heighten concern. The Sentencing Bill 2025 proposal (Clause 35) to allow probation to publish names and photographs of people on community orders online formalises "naming and shaming" and risks creating yet another layer of digital permanence, with no clear rules on duration, delisting or deletion. Advances in AI, including facial recognition and automated data scraping, further threaten the effectiveness of traditional protections such as name changes.

In response, Unlock recommends a programme of digital rehabilitation reform, including:

- Modernising the ROA to include explicit digital rehabilitation provisions and a presumption of delisting once convictions are spent.
- Statutory guidance clarifying a consistent public interest test for retaining historic conviction data online.
- A specialised Digital Rehabilitation Tribunal for serious offences to review risk, rehabilitation and proportionality on a case-by-case basis.
- Compliance with ethical standards on reporting spent convictions, aligned with IPSO and ICO protections.
- Strengthening ICO capacity and tools to act swiftly against vigilante sites and unlawful data processing.
- Public awareness campaigns and accessible tools (e.g. template letters) to help individuals use ICO and IPSO remedies.
- Clear regulatory standards for AI-generated or AI-processed criminal record data.



Our briefing concludes that rehabilitation is not about erasing the past, but about recognising people's capacity to change. Fifty years after the ROA, the internet has turned formal and legally protected second chances into a conditional privilege controlled by algorithms and tech platforms. Without urgent action, the UK's promise of rehabilitation will remain, for many, a legal fiction rather than a lived reality.



Background

The Rehabilitation of Offenders Act (ROA) came into force 50 years ago, introducing a right to be rehabilitated. Under the ROA, most sentences or disposals have a 'rehabilitation period' during which a caution or conviction is considered 'unspent'. Once the rehabilitation period ends, a caution or conviction becomes spent. Before something is spent, an individual would have to disclose it when asked such as during recruitment processes, applying for higher education or to get insurance.

Once a caution or conviction becomes spent, it is only disclosable in specific circumstances. This is generally in relation to employment or when applying for specific permissions or licences. These are set out in the ROA Exceptions Order[1]. Some common professions where a spent caution or conviction may still be disclosed include nursing, social work, and teaching. You can read more about the ROA Exceptions Order on Unlock's website.

When applying for these specific roles individuals would be required to disclose both spent and unspent cautions and convictions unless they are protected under the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975 (Amendment) (England and Wales) Order 2020.

Basic

In reality any employer can request a basic check. For example, government roles would usually carry out a basic check, as might roles in the travel industry. It is also used in other situations e.g. insurance claims where you might need to provide proof of your unspent convictions. This level of check shows any unspent cautions and convictions.

[1] The Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975

Standard

Employers recruiting for certain positions can request standard checks. These may be for people wanting to be approved by the Security Industry Authority (SIA) or anybody applying to become a solicitor or barrister. Such checks show both spent and unspent cautions and convictions unless they are protected.

Enhanced

This check is also for employers recruiting for certain positions exempt from the protections of the ROA, as well as those listed in regulations made under the Police Act 1997. Such checks are usually for employment or voluntary positions which include frequent or intensive contact with children or vulnerable adults, such as teachers, doctors, or social workers. In addition to the information provided in a standard check they also show whether a person is barred from working with children and/or adults. Relevant information from local police records can also be provided.

This robust process, in addition to the barring lists (which identify when a person is prohibited from working in certain regulated roles and where inclusion does not necessarily indicate a criminal record) means that core safeguarding processes are not undermined by a record becoming spent. The Disclosure and Barring Service (DBS) process therefore is twofold; allowing people to move on once their sentence and rehabilitation period is completed, and ensuring important information is shared when necessary. This principle is fundamental in supporting people to move on with their lives.

How is criminal record data available online?

Information about criminal records generally appears online via news articles and social media. Some local news outlets post regular lists of people convicted in regional courts. Some offences may reach the news, local or national, as a distinct news story. Criminal record data can also be found online in other, sometimes surprising ways. For example, via our helpline we know of one prospective employer searching professional legal databases to find out if applicants had ever been to court.

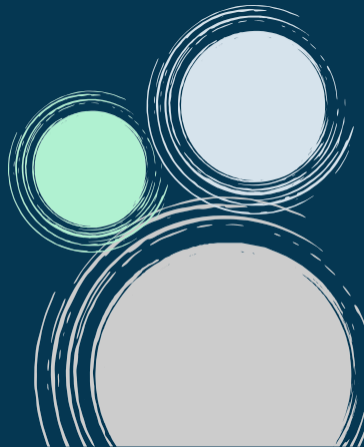
Search engines make this type of digital content easy to find. When the ROA was passed into law in 1974, this availability of information would have been inconceivable. The ROA's legal protections were designed in a world in which an employer would find out about criminal records only by asking an applicant. This is reflected in systems such as the DBS. An employer must seek the consent of an applicant to request a DBS check; it is not something the employer can do on their own terms without approval from the individual concerned. Yet, today, an employer may be able to find data about someone's criminal record that they would not even have access to via a DBS check.

The key issues

Every year we hear from hundreds of people for whom the internet has had a huge impact on the disclosure of their criminal record. This can undermine one of the main aims of the ROA; that in most circumstances, people are not required to disclose their criminal record.

When the ROA was passed in 1974, it existed in a world radically different to the one we live in now. In restricting employers', and others', access to criminal records information, the writers of legislation assumed a world in which those wanting to know about someone's criminal record would have to ask that person directly. They didn't envisage a world in which they could look up billions of lines of information online. The internet has had a profound impact on the protections of the ROA and a deep impact on the notion of a protected second chance.

Our website receives over 1.4 million visits annually and our helpline responds to over 10,000 calls over the same period. Criminal records being exposed in internet searches is a commonplace query for our helpline. People contact us seeking advice and support on how to respond when an employer or other organisation holds criminal records information that was acquired through an online search. At Unlock we regularly provide people with advice on how to respond to employers who have access to information found online and also how to apply to have online information about themselves removed. Often this online information is outdated and inaccurate. You can read Unlock's advice page here.



Prospective employment

We know that many hiring managers routinely use online searches in the recruitment of prospective staff. This poses a clear risk to the protections laid out in the ROA. These searches can often take the form of basic search engine usage, large language model searches (ChatGPT) or social media trawling. These may be conducted as background checks, but these can seriously discriminate against those with both spent and unspent convictions. This is problematic for the following reasons:

- Online information about someone's criminal record is likely to be incomplete, based as it often is on news reporting rather than official records. A news organisation might report one court case and not another, perhaps even failing to report on an acquittal whilst reporting a charge. No one should rely on an internet search to gain holistic information.

- Online searches can undermine the ROA and give employers access to information to which they are not legally entitled. This could place them in breach of data protection legislation as well as breaching the protections inherent in the ROA – they may have information about spent convictions which is not relevant to the role they are recruiting for. They may, also, have collected this data excessively, not to say duplicitously.

- This problem is unlikely to impact all people with criminal records equally. Online searches are likely to be far easier to conduct for those with non-anglicised names. There can be a discriminatory element to this – with names that are less common in the UK being easier to find. This compounds an existing problem – Nuffield College research shows that less anglicised names are more likely to be excluded by employers.[2] **Therefore people with criminal records who have less common names face double discrimination.**[3]

[2] New CSI report on ethnic minority job discrimination, Nuffield College Oxford University
[3] Internet searches on job applicants add to double discrimination for people with non-anglicised names - Unlock

- Women are also more likely to be found online due to increased media interest in their involvement in the criminal justice system. Our previous research in 2021, supported by the Barrow Cadbury Trust, found that women often face lasting exclusion from employment and volunteering due to online records linked to past trauma, poverty, or minor offences. Women can also be especially vulnerable to being tracked down by abusive former partners.

- Digital imprints also affect the person's family, friends and wider networks. Children can be especially vulnerable to bullying with a parent who is searchable online.

- Lasting psychological harm can be caused through heightened anxiety, depression, fear of community hostility, social isolation and withdrawal from pro-social activities.

- Living in this Long Shadow of a criminal record can erode trust in legitimacy of state institutions and increase the risk of people disengaging altogether from civil society and negatively affect reoffending rates.

> What happened to me in court was published online. This has led to me being fired from a job after someone at work googled my name - this happened 15 years after the conviction.
>
> I've also lost relationships due to partners and potential new friends googling my name. My overall confidence was eaten away and this led to me spending a lot of money on dealing with my shame in therapy.

The Sentencing Bill 2025, Clause 35 - naming and shaming

On 12 September 2025, the UK Government announced plans – as part of its sentencing reforms – to give the probation service powers to publicly publish the names and photographs online of people on community orders. Ministers argue this will increase public confidence in community sentences. At the time of writing, no clear guidance has been issued on how long these identifiers will be available online, if they will be delisted or deleted and how the information will be stored. This new move to name and shame will have many significant impacts long after a criminal record is spent.

Our work clearly demonstrates risks in the experience of online visibility and reinforces the importance of protecting mechanisms like the right to change one's name. A name change can sometimes be the only way to avoid the impact of internet searches and protect a person's right to move on. But with the growth of AI photo recognition tools, even a name change cannot guarantee that a spent conviction will remain in the past.

> My conviction is never spent because google always has it. I think once a conviction is spent to truly be spent the law needs to change so google has to remove it if requested and not be the decision makers as to whether it's in the public interest. In the eyes of the law, you are allowed to get on with life but google makes that impossible.

Rogue sites and digital records

Alongside official measures, there is a murkier ecosystem of vigilante-style or rogue 'naming and shaming' sites such as ‘Red Rose’. These platforms claim to act in the ‘public interest’ by exposing people with past convictions, often using language about community safety or transparency. In reality, they operate entirely outside legal frameworks or due process. Using simple AI technology, they dredge up old and sometimes spent convictions, then publish personal information in ways that can follow people indefinitely. By framing their activity as serving the public good, they exploit a grey area: while their actions have no legal authority, search engines often index their content alongside legitimate journalism, amplifying harm and undermining rehabilitation.

Collection and retention of personal data

The internet effect can be a particular problem for people with criminal records seeking employment, education or volunteering opportunities. As outlined above, many applicants' criminal records do not need disclosing for most roles or courses. Yet, when applying for these opportunities, people with criminal records may not be able to expect their right to non-disclosure to be upheld. This is because many organisations conduct internet searches on candidates during recruitment or enrolment. News articles and social media posts do not differentiate between 'spent', 'unspent' or protected ('filtered') criminal records.[4] Therefore, organisations searching candidates online may learn about a criminal record irrespective of the person's right to not disclose it.

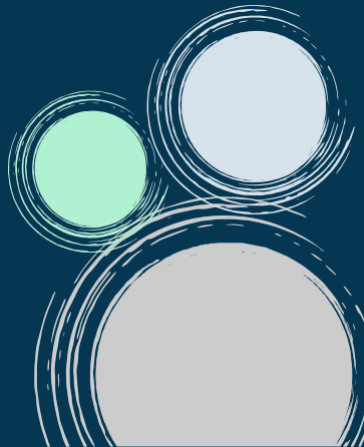
Collection and retention of data on unspent convictions can only be conducted when there is a legitimate basis for doing so. Employers may not specifically be searching for criminal record data when they conduct an internet search, but may encounter it, nonetheless. If this happens, many employers will not have considered how to deal with the data and will not have evidenced that they have a legitimate basis for collecting it. Internet searches on candidates are likely to also reveal other sorts of sensitive data. This could include information about an applicant's personal and family life, disability status or sexuality. There is, therefore, substantial compliance risk to organisations who conduct internet searches on applicants, particularly if they process sensitive or criminal offence data without a lawful basis, in breach of UK General Data Protection Regulation (GDPR). Employers must have a lawful basis for collecting and processing personal data – including data discovered through internet searches. If data is collected about an applicant or employee, there has to be a lawful basis for collecting it, storing it and sharing it.

[4] https://unlock.org.uk/advice/what-will-be-filtered-by-dbs/

An additional complication is that news stories can include inaccuracies. Even small errors or misrepresentations can pose significant challenges for the subject of an article. Having a significant incident in one's life mischaracterised is challenging on a personal level. Practically, this also means the way that the individual discloses their criminal record will differ from how it is reported publicly.

We know that organisations use internet searches to 'corroborate' a person's criminal record disclosure. Many then assume that where there are discrepancies the person must have been dishonest. This is unfair and unjust considering the complexity of the criminal record disclosure regime. In most cases people who don't disclose fully have made a genuine mistake. Yet, in the case of inaccurate criminal record data online, the subject of an article will not be able to disprove this presumption of dishonesty all the time the article remains online. The only official, reliable source of data regarding criminal records is a DBS certificate (provided it has been requested and processed at the appropriate level).

Unfortunately, the difficulties posed by searchable criminal record data doesn't stop at the point of application or joining an organisation. We hear from people who are already in post, or have started on a course, whose colleagues or peers have 'discovered' their criminal record online. In this situation, some people choose (or are forced) to leave their job or course because of stigmatisation or harassment – with no clear redress under the Rehabilitation of Offenders Act.



Ethical journalism

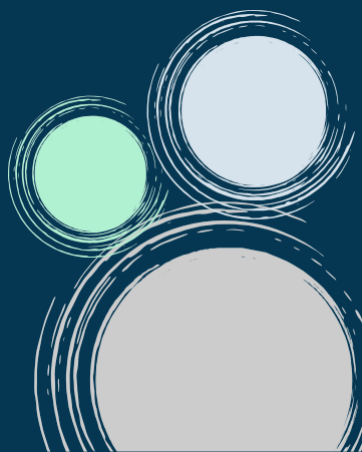
Sensitive, responsible reporting on criminal justice can deepen public understanding, challenge myths, and inspire positive change. Ethical judgment lies at the heart of journalism—and defines how reporters see their role in a democratic society.

In an age where anyone can publish, journalists often point to professional standards to argue that not everyone can be a journalist. Yet such standards in relation to criminal records reporting are ignored. Sensationalism, unchecked bias, and breaches of the protections of the ROA erode credibility and compassion. The result? Shallow, distorted stories that neglect both truth and the human toll behind it.

In the context of the Right to be Forgotten, ethical journalism has a crucial role in preventing the unnecessary circulation of historic criminal records. The Independent Press Standards Organisation (IPSO) Editors' Code of Practice (https://www.ipso.co.uk/editors-code-of-practice) provides safeguards that are directly relevant. It requires journalists to avoid publishing misleading or outdated information, meaning reporters should clarify whether a conviction is spent under the Rehabilitation of Offenders Act 1974 and avoid presenting old offences as current fact. It also prohibits prejudicial or pejorative references to a person's past unless genuinely relevant to the story, while IPSO guidance on privacy reminds editors to avoid unjustified intrusion into the lives of individuals.

[4]https://unlock.org.uk/advice/what-will-be-filtered-by-dbs/

Ethical reporting therefore requires the media to consider the real-world harms of resurfacing old convictions, including risks to safety, employment, housing and rehabilitation. Where reporting breaches these standards, IPSO can require corrections or apologies of material. In a digital landscape where news articles are searchable indefinitely, adherence to IPSO standards is a necessary safeguard against perpetual stigma, and aligns journalism with the principle that people should not be punished forever for past offences that are now spent.



The law and the right to be forgotten

A case ruled in the Court of Justice of the European Union (CJEU) in 2014 created a potential remedy for people impacted by the internet effect. It established that search engines could be compelled to 'delist' certain search results relating to EU citizens.

This is informally known as the 'right to be forgotten', frequently tied to Article 17 (GDPR) right to erasure. The 'right to be forgotten' states individuals have the right to have their personal data erased if:

- it is no longer necessary for the purpose for which it was originally collected
- an organisation relies on consent to hold the data and the individual withdraws their consent
- the data has been unlawfully processed
- the individual objects to the processing and there are no overriding grounds for continuing it
- the data must be erased to comply with a legal obligation
- the data relates to a child and was collected in connection with offering online services.[5]

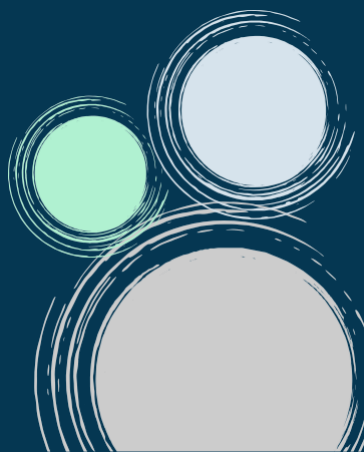
UK GDPR is the main law that governs how personal data must be collected, stored and used. It gives people rights over their personal information and places legal responsibilities on organisations that hold it. One of those rights is the ability to ask for personal data to be deleted in certain circumstances, such as when it's no longer needed or is causing harm.

[5]Right to erasure | ICO

These provisions are interpreted through landmark cases such as Google Spain SL & Google Inc v AEPD and Mario Costeja González (C-131/12), which first confirmed that search engines are data controllers responsible for delisting requests.

A UK court case in 2018, 'NT1 & NT2 v Google (2018)' saw two men with historic convictions bringing claims under the Data Protection Act. They argued that their offences should no longer define them online. In one case, the judge refused de-listing because the claimant had shown little remorse and his business interests made the conviction still relevant. In the other, the claimant won: the offence was historic, rehabilitation was clear, and disclosure was deemed disproportionate.

Together they form the framework used by search engines, regulators, and courts to decide whether continued indexing of personal information remains lawful and proportionate under UK GDPR.



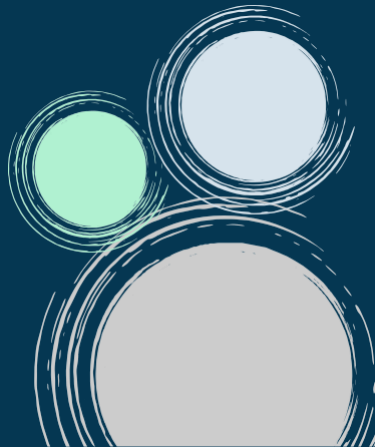
The challenge of delisting

For an individual, the process of requesting delisting can be complex and opaque. There are numerous search engines, and a person needs to apply to each separately. If successful, delisting only removes the search engine results; it doesn't remove the data at source. The publisher of the information e.g. the newspaper must then be contacted separately with a request for removal.

A conviction being 'spent' – meaning it no longer needs to be disclosed under the Rehabilitation of Offenders Act – is often the starting point for arguing that the information no longer meets the public interest and should no longer appear in search results.

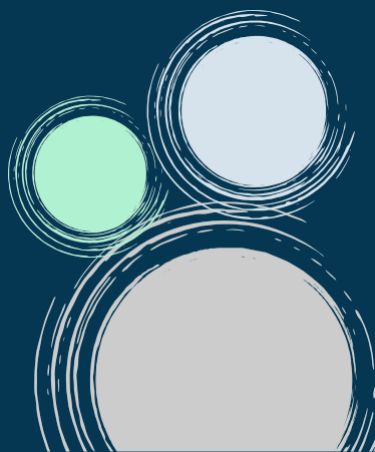
However, this is not always a reliable remedy; it can be challenging to predict whether a request for delisting will be approved. The criteria used to assess someone's request generally relate to public interest in access to the data. For example, this could take account of whether someone was convicted of a crime whilst in a profession in which they still work. If their criminal record is spent, but the search engine company determines that it is still in the interest of the public to know, they may reject the request. It isn't always clear how decisions are reached and why some records are considered relevant to the public where others are not.

In 2023, 22% of all UK delisting requests made to Google related to content on crime. Most UK requests for crime data delisting (37%) were directed to news sites. The sites from which Google has approved delisting the most are Twitter/X, Facebook and the Daily Mail website.



Even where the search engine agrees that the coverage of a crime is out of date, they may not remove all links. In one example, a person was acquitted of a crime. Google delisted the articles detailing the original charges and proceedings on the basis that they had since become outdated. However, Google refused to delist a more recent article which gave details of the alleged offence but explained that the person was acquitted. For the subject of this article, the effect of having these charges searchable online, remains the same.

If delisting requests are unsuccessful, or do not fully resolve the impact of the internet effect, alternatives are out of reach for most. Legal action to challenge a publisher is likely to be both costly and lengthy.

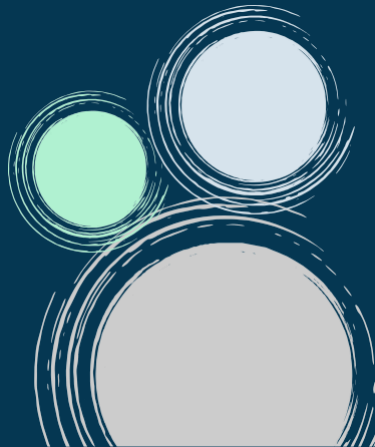


Information Commissioner's Office

The Information Commissioner's Office (ICO) is the UK's independent regulator for data protection and information rights, responsible for enforcing laws including the Data Protection Act 2018 and the Freedom of Information Act 2000. It focuses on areas where non-compliance could cause the greatest harm.

The ICO has distinct regulatory powers to intervene where criminal conviction data is inaccurately recorded, published, or retained. Data controllers are required to ensure that such information is accurate, up to date, processed lawfully and fairly, and not kept or disclosed for longer than is necessary.

Misreporting of criminal records data, including incorrect offence details, attribution to the wrong individual, or the continued publication of spent criminal records may breach core data protection principles. Where organisations fail to rectify or remove inaccurate information on request, individuals may escalate complaints to the ICO. The ICO may issue enforcement notices, require erasure or correction, restrict further processing, or impose financial penalties. While media organisations and journalists benefit from certain exemptions for public interest reporting, these do not extend to knowingly false or reckless publication, and the ICO retains the authority to act in cases of demonstrable inaccuracy. As such, the ICO provides an important regulatory route when inaccurate or misleading criminal record information causes ongoing harm.

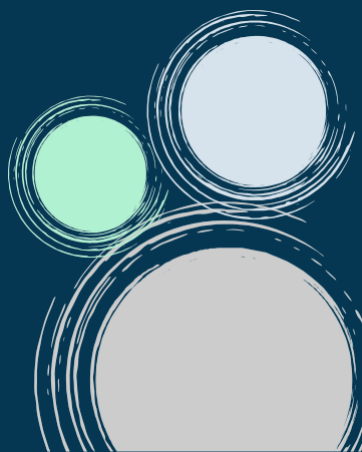


In recent years, "vigilante sites" – websites or social-media pages publishing names, photographs, and alleged offences – have become a serious concern. Often featuring people with past convictions or unverified allegations, these platforms operate outside lawful data-processing standards, causing distress, reputational damage, and sometimes real risk to life.

Claims of acting in the public interest should not excuse unlawful handling of criminal records. While the ICO has broad powers, the proliferation of such sites on social media, sometimes based outside of the UK, means that actions remain slow and complex.

An individual can complain to the ICO about mishandling of their criminal record data, but we are concerned about procedural delays affecting its ability in tackling serious breaches and ensuring compliance.

To protect individuals and restore trust, urgent reforms are needed to strengthen enforcement and make GDPR protections truly effective.



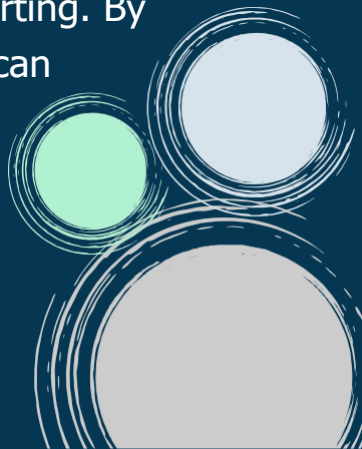
Unlock recommends

Modernise the Rehabilitation of Offenders Act (1974)
To include digital rehabilitation provisions that presume delisting once a criminal record is spent and clarify responsibilities and thresholds for delisting.

Clarification of the public interest threshold
Issue statutory guidance on 'public interest': There is currently no consistent test of when historic criminal record data remains in the public interest and when it does not. At present, tech companies make such decisions with minimal transparency, and individuals can only escalate to the Information Commissioner's Office (ICO) or to the courts which is arduous. We need UK-level guidance – developed with Ministry of Justice, the ICO, civil society and people with lived experience – that presumes rehabilitation unless specific, evidenced risk outweighs it.

Case-by-case review for serious offences
Development of a Digital Rehabilitation Tribunal for the most serious offences. There should be a structured and reviewable process to weigh rehabilitation, time elapsed, current risk, and relevance to public interest. This should include a formal route to demonstrate change and seek proportional relief.

Clear ethical standards for reporting
Media outlets promote clear ethical standards for reporting on criminal justice issues. Journalists should be supported to challenge bias, avoid sensationalism, and highlight the human impact of their reporting. By embedding these principles in everyday practice, journalism can strengthen public trust and demonstrate leadership in responsible journalism.



Sector specific guidance

Many online news archives, search engines, and third-party data platforms remain unclear about their obligations when conviction data is outdated or inaccurate. The ICO should publish sector-specific guidance setting out reasonable expectations for accuracy checks, review periods, takedown procedures, and the handling of spent convictions.

Strengthening ICO

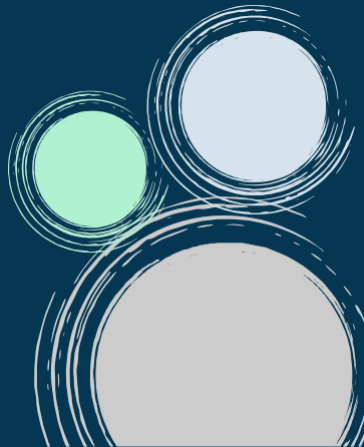
Strengthen the ICO to enable swift, joint action for the removal of vigilante content.

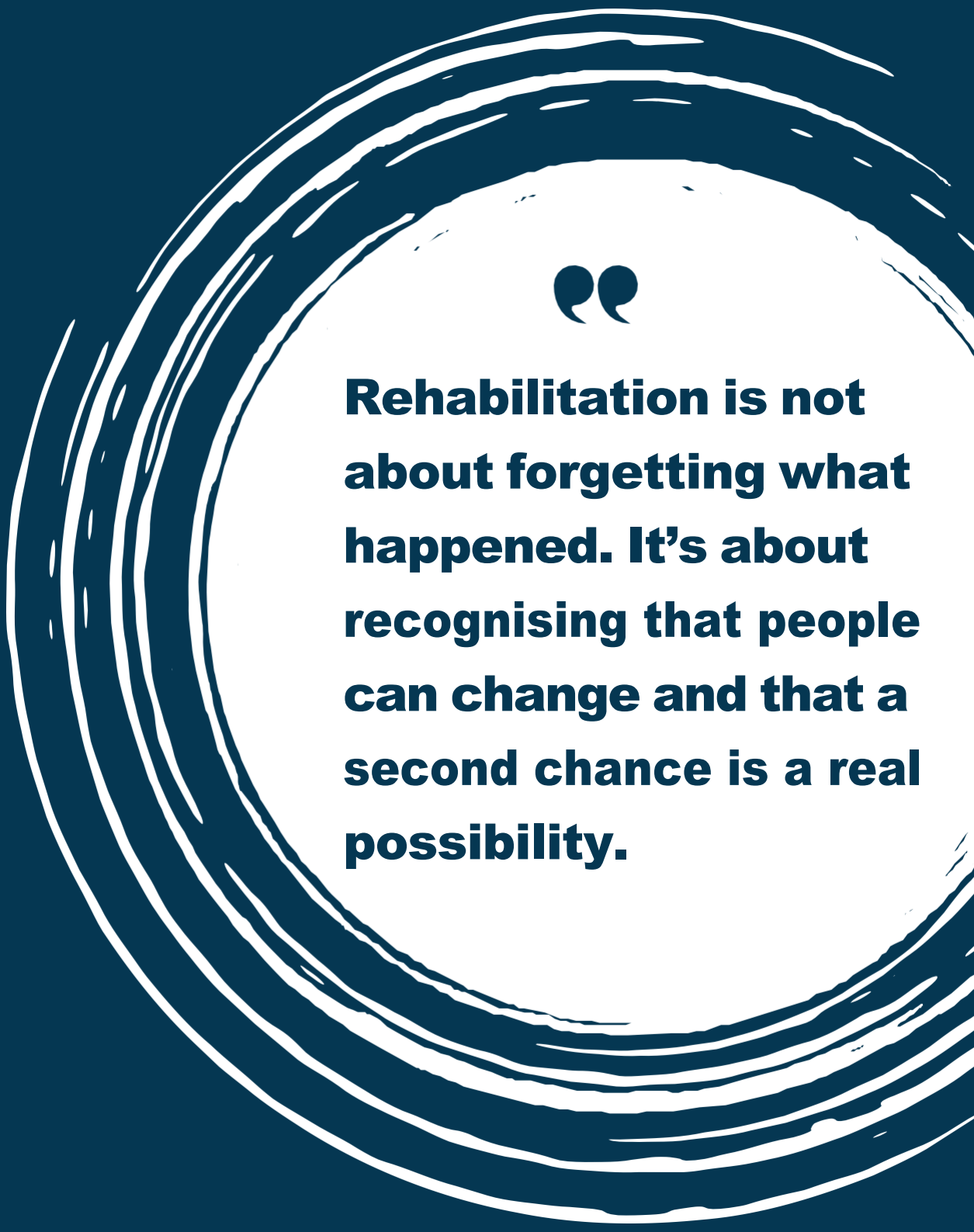
Raising public awareness

Increase public awareness of ICO and IPSO complaint procedures and promote understanding of victims' rights to data removal, redress, and compensation. Many individuals do not know they can challenge inaccuracy or seek erasure of outdated conviction data. The ICO and IPSO should lead on targeted public awareness campaigns and provide accessible template letters and guidance for people seeking rectification or removal.

Clear standards for AI generated or processed information

Establish clear regulatory standards for the collection, use, and sharing of information generated or processed by AI systems, ensuring transparency, accountability, and proportionality in data handling.



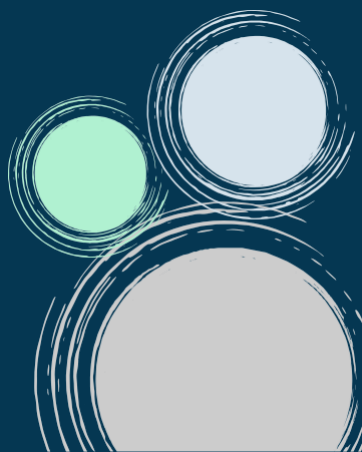


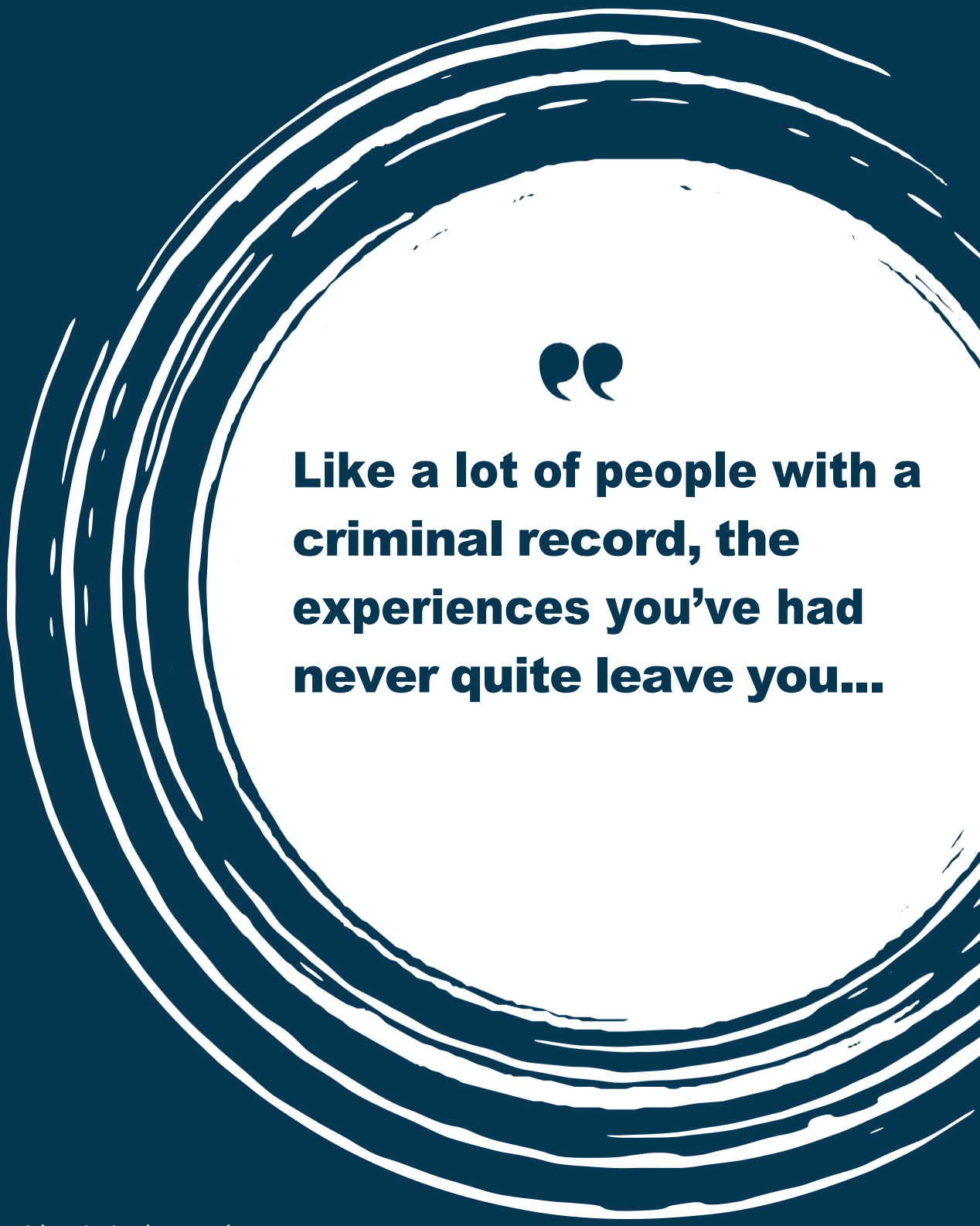
Rehabilitation is not about forgetting what happened. It’s about recognising that people can change and that a second chance is a real possibility.

Conclusion

Half a century ago, the Rehabilitation of Offenders Act promised citizens a second chance. In the internet era, that promise has decayed into an illusion. Today, rehabilitation depends not on conduct but on algorithms.

The **digital afterlife of conviction** perpetuates stigma, exclusion, and despair. It undermines public safety by denying people the conditions in which desistance flourishes - employment, belonging, and hope.





Like a lot of people with a criminal record, the experiences you've had never quite leave you...

Unlock, for people with criminal records
Published 11 December 2025
www.unlock.org.uk
Charity no. 1079046
Companies no. 3791535