UNITED KINGDOM

Tools	ChatGPT | DocDefender | Domestic Abuse Risk Assessment Tool | Harm Assessment Risk Tool | Luminance AI | Microsoft Copilot | Offender Assessment System | Offender Group Re-Conviction Scale | PredPol | Qlik Sense | Specialised systems
Tasks	Case management | Data review and analysis | Evidence review and analysis | Legal research, analysis and drafting support | Operational support | Predictive analytics
Users	Law enforcement | Prosecutors | Courts | Defence
Scope	Nationwide
Training	No mandatory or systematic training
Regulation	There are no express statutory regulations on the use of AI in criminal proceedings, but several bodies have issued guidelines on AI use by legal practitioners and existing laws regulating criminal procedure and data protection may be construed to regulate the use of AI (Police and Criminal Evidence Act 1984, Equality Act 2010, the Data Protection Act 2018 and UK GDPR)
Cases	Courts have recently ruled on a number of "hallucination" cases; found the use of automated facial recognition technology by the South Wales Police to be unlawful; and endorsed the use of AI in the context of electronic disclosure in civil proceedings
Insights	'Soze', an AI system trialled by Avon and Somerset Police in 2024 to solve decades-old cold cases, was able to sift through the evidence in 27 complex cases in just 30 hours, a task that would take over 80 years for a human to do

AT A GLANCE

In the United Kingdom, at every stage of the criminal process, at least one actor is using AI in some form, though the extent and complexity of its deployment vary. For instance, English police forces are using AI for predictive analytics, including to predict the likelihood of offenders reoffending, and for facial recognition or automated redaction. Courts are using AI for case management, and (increasingly) for legal research, analysis and drafting support. As of September 2025, the first English judge has disclosed his use of AI to assist in producing a judgment. Defence counsel have used AI for evidence discovery and disclosure in criminal trials, including to analyse and identify key evidence and individuals of interest.

Despite this scope of use, there are no statutory regulations governing the use of AI in criminal proceedings, as at September 2025. However, several professional bodies have issued AI guidelines for legal practitioners, including the Courts and Tribunals Judiciary, the Bar Council, the Law Society and the Solicitors Regulation Authority. Law enforcement agencies have likewise published a set of principles to guide the use of AI in policing. In addition, existing general laws, such as the Police and Criminal Evidence Act 1984, the Equality Act 2010, the Data Protection Act 2018 and the UK GDPR may limit the use of AI and AI-generated material in courts. English courts, meanwhile, have in a series of recent cases addressed the misuse of AI by litigants in non-criminal proceedings and examined the lawfulness of automated facial recognition and technology-assisted evidence review.

The United Kingdom can be divided into three legal systems: England and Wales, Scotland, and Northern Ireland. The AI Justice Atlas focuses on England and Wales unless it is expressly stated that the position applies to the entirety of the United Kingdom. Where indicated, certain points also address the position in Scotland.

USE

At every stage of the criminal process, at least one actor is using AI in some form, though the extent and complexity of its deployment vary. In Scotland, the use of AI in law enforcement and by prosecutors is being explored.

LAW ENFORCEMENT

A 2024 underline survey of nine English and Welsh police forces by the Police Foundation found that those forces are currently using or considering using AI technologies in the following areas:

1.
    1. **AI for operational support:** assistance for back-office support functions; resource allocation (officer and vehicle); and optimising investigative timelines;
    2. **AI for predictive analytics:** risk management of warrants; minimising the likelihood of crime; health warnings; and anticipating future crime trends and hotspots;
    3. **AI for data review and analysis:** redaction; lie detection; facial recognition; identifying patterns across cases; technical examination of data.

Operational support

Data from 2016-2019 underline suggests that at least **15% of police forces in England and Wales** have used algorithmic decision aids, although the proportion has likely increased since that research was conducted. In 2023, the National Police Chiefs' Council underline stated that all UK police forces use data analytics and **15 forces use advanced data analytics**, with most AI applications being used for organisational effectiveness and workplace planning (such as triage of 999 (emergency) calls and automation of administrative tasks).

One example is police forces using AI for operational support. Bedfordshire Police, for instance, has adopted an underline automated approach (using robotic process automation) to **requests for authority**, such as where a chief officer must provide authorisation before an operational

deployment of firearms or directed surveillance. With this automation, the process that previously took four hours per authority is now completed in one minute.

Chatbots are also being used by police units for **public contact**. Bedfordshire Police uses chatbots to handle issues such as claims for small-scale robberies and property damage, and requests to help trapped or endangered pets. 20% of queries to Bedfordshire Police are now answered by chatbots.

Natural language technologies (tools that can understand and work with human language) are also being trialled that can triage and provide initial responses to either text or voice content, including an identification of emotions such as stress and fear in callers' voices.

Predictive analytics

The **Offender Assessment System** (OASys) is a tool used to **assess the risk of harm and re-offending**, and inform decision-making about both sentencing and parole, which nowincorporates AI techniques to profile thousands of offenders every week. According to the National Offender Management Service, OASys uses a combination of 'structured professional judgment' and risk prediction algorithms to generate 'risk scores'. These risk scores are the 'most influential document' in the sentence, planning and management process, and are used to inform decisions on bail, sentencing, the type of prison to which someone will be sent, and access to education and rehabilitation programmes. Figuresfrom January 2025 show that 9,420 assessments were completed in one week, and more than 1,300 assessments every day.

OASys assessment considers some risk factors that are static (unchangeable) such as criminal history and age, and others that are dynamic (changeable) such as accommodation, employability, relationships, lifestyle and associates, drug misuse, alcohol misuse, emotional wellbeing, thinking and behaviour, and attitudes. Different weights are assigned to different risk factors (criminogenic needs), correlating to their greater or lesser predictive risk. A human assessor then uses discretion in providing an overall score for the dynamic risk factors. Finally,

the system adds data about an individual's offending record as well as offender demographic information and assesses <u>two</u> outcomes: likelihood of violent re-offending and the likelihood of non-violent re-offending.

The Prison and Probation Service <u>found</u> in 2015 that the OASys General reoffending Predictor (**OGP**) and OASys Violence Predictor (**OVP**) predictive algorithms generated different predictions based on gender, race and age. In particular, the predictive tools were better at forecasting reoffending by women, white offenders, and older people. For racialised groups, especially Black and mixed ethnicity offenders, the predictions were less accurate. Whilst OASys is subject to cyclical reviews by HM Inspectorate of Probation, there has not been an official published review of the system since 2015.

> "Relative predictive validity was greater for female than male offenders, for White offenders than offenders of Asian, Black and Mixed ethnicity, and for older than younger offenders. After controlling for differences in risk profiles, lower validity for all Black, Asian and Minority Ethnic (BME) groups (non-violent reoffending) and Black and Mixed ethnicity offenders (violent reoffending) was the greatest concern."
>
> *National Offender Management Service, 2015*

The HM Prison and Probation Service Assess Risks, Needs, and Strengths (ARNS) project is <u>developing</u> a new digital tool to replace the OASys tool which has been piloted since December 2024 with a view to national rollout in 2026. The tool will deliver an 'organisational change in the approach to how assessments, risk management and sentence planning are undertaken in practice', enabled by a new digital service.

Another predictive tool used in conjunction with, or as an alternative to, OASys is the **Offender Group Re-Conviction Scale** (OGRS) tool. OGRS attempts to predict an individual's likelihood of reoffending within two years by using data on an individual's age at sentence, gender, their number of previous criminal sanctions (cautions and convictions), their age at first sanction, and current offence, alongside a 'copas' rate (the volume and speed of an alleged criminal 'career'). OGRS includes separate predictors of violent reoffending and non-violent reoffending.

Together, the OASys and OGRS tools can be used at both pre- and post-conviction stages:

Pre-conviction stage	Post-conviction stage
1. A case is adjourned for 15 days to get a full report based on an OASys assessment. 2. On the day reports, five-day reports, and oral reports can also be based upon an OGRS assessment.	1. If, on conviction, the likely sentence for an individual for their offence is less than two years, the OASys assessment, as part of the pre-sentence report, can influence the choice between a custodial sentence and a community order. 2. In probation hearings, a 'low' risk score can often mean that an individual will be released 'on the papers', without a need for a hearing.

The **National Data Analytics Solution** (NDAS), introduced in 2016, was created by the Home Office and local police units. It uses machine-learning and predictive analytics to conduct behavioural analysis and predictive modelling in order to create and provide individual predictions and profiles about individuals and their likely future action, which are then intended to inform and influence pre-emptive policing interventions. NDAS uses data from each participating police force, including police intelligence reports on individuals and events, stop

and search data, drug use data and custody information. One example of an NDAS model that was previously developed is a model aimed at predicting 'most serious violence' (MSV). The MSV model, intended to be trained using machine learning, aimed to predict which individuals already known to the police are likely to commit their first most serious violence offence with a gun or a knife within 24 months. However, the MSV model faced various challenges, including as regards its accuracy, and was subsequently abandoned without ever being used by the police. It is unclear whether a new version or other aspects of NDAS are currently in use by the police force.

Several local law enforcement agencies also harness AI for predictive policing in relation to both suspects and victims:

Avon and Somerset Police	Avon and Somerset Police use programmes that can predict the likelihood of an individual's victimisation and vulnerability; of their being reported missing; of them falling victim to stalking and harassment; and of them being a victim of a serious domestic or sexual violence.
	Tools have also been used to predict the likelihood of a suspect re-offending and perpetrating: stalking, harassment, and serious domestic or sexual violence. Avon and Somerset Police has been using algorithms through its system called Qlik Sense since 2016, and it has said that there have been around 300,000 people on its internal Offender Management App, and that as many as 170,000 people have been profiled and assigned a risk score over the past six years.
Durham Constabulary	From 2015 to 2021, Durham Constabulary used the Harm Assessment Risk Tool (HART), a machine-learning model developed by Durham Constabulary in partnership with Cambridge University starting in 2017. HART is a form of supervised machine learning

which uses an algorithm that combines the results of many decision trees analysing 34 variables (such as age, gender, arrest history, and postcode) to classify arrested individuals at low, medium, or high risk of committing a violent or non-violent offence in the next two years. Individuals considered low or medium risk were eligible to participate in a 'Checkpoint' rehabilitation programme, which if completed would allow them to avoid charge and prosecution. However, according to the Police Foundation, the HART tool deployed by Durham Police exhibited various flaws, for instance over-estimation of the likelihood of re-offending and discrimination in the data. Durham Constabulary ceased the use of the HART tool in 2021.

Hampshire and Isle of Wight Constabulary and Thames Valley Police	The Domestic Abuse Risk Assessment Tool (DARAT) uses information gathered by the attending officer at a domestic abuse case as well as any available historic data relating to the people involved to predict the likelihood of further harm occurring in the year following the incident. The prediction falls into three categories: standard risk, medium risk, and high risk. The current status of DARAT is unclear, with some sources suggesting that DARAT is still in development, and other sources suggesting that it is now being used by police.
Kent Police	Kent Police previously used PredPol, software developed by a US firm to predict where and when crimes would occur, for five years until 2018. However, the costs of the software, at £100,000 per year, were deemed too high, and the software was subsequently withdrawn from use.

Oxford Institute
of Technology and Justice

AI tools are also used by police to deliver facial recognition technology. There are three types of such technology in regional use or development in England and Wales:

1. **Live facial recognition (LFR)**: involves a camera scanning a scene and checking facial images against a database of wanted individuals. LFR cameras are typically used to identify persons wanted for homicide, rape and serious violence, as well as persons wanted by the courts.

2. **Retrospective facial recognition (RFR)**: involves reviewing images or videos taken from CCTV, dashcams, mobile phones, social media, and video doorbells. These images are compared to arrested individuals to verify identity or help to identify the missing and deceased.

3. **Operator initiated facial recognition (OIFR)**: allows officers to photograph a person of interest in order to verify their identity.

It has been <u>reported</u> that civil servants are working with police forces to develop a new **nationwide** facial recognition system, known as Strategic Facial Matcher. This platform will be capable of searching multiple databases, including custody images and immigration records.

> 🔍 Closer look
>
> While police forces in England and Wales have been trialling facial recognition since 2016, there has <u>been</u> a significant escalation in its use over the past year, with live facial recognition becoming a routine feature of policing practice. In 2024 alone, approximately 4.7 million faces were scanned by police, more than twice the number recorded in 2023. Live facial recognition vans were deployed on at least 256 occasions, compared to just 63 in the previous year.

The Home Office has **Oxford Institute** provided <u>funding</u> for work carried out by the Police Digital Service to *of Technology and Justice* design and deliver automated text redaction frameworks, which will enable the administrative task of text redaction to be undertaken **much more effectively.** Forces can now procure from four suppliers, who have qualified to be part of the framework. It is expected that the solutions will reduce the amount of time required to deal with redactions by up to 80%.

In Scotland, Police Scotland <u>announced plans</u> in August 2025 to introduce live facial recognition technology.

Some forces are also using counter-proliferation <u>Internet of Things</u> (IoT) device forensics, whereby software can analyse images and determine the location of a potential victim of human trafficking or a missing person.

Local law enforcement agencies in England and Wales also harness AI in their data review and analysis:

Avon and Somerset Police	In 2024, Avon and Somerset Police were <u>trialling an AI system</u> to help them solve decades-old cold cases. The system, called Soze, was able to sift through the evidence in 27 complex cases in just 30 hours, a task that would take over 80 years for a human to do.
Bedfordshire Police	Bedfordshire Police has pioneered the use of <u>DocDefender</u> to auto-redact documents (for example, personal information and information describing other data such as how it was collected and who collected it) before they are sent to the Crown Prosecution Service.

In June 2025, the Crown Prosecution Service (CPS) published its **mission statement on how it will use AI in the future.** Some of the key elements of that mission statement include a commitment to ensure that AI will be overseen by humans and promoting transparency on the use of AI by the CPS. In June 2025, the CPS announced a government Spending Review that increased the CPS' funding by an additional £96 million between 2026 and 2029 which will be dedicated to, among other things, 'unlocking digital developments through AI'.

Case management

A pilot of Microsoft Copilot within the CPS concluded in August 2024, with over 400 staff across the organisation given access to Copilot to assist them in everyday tasks, for example summarising emails and analysing excel data. The scheme established that Copilot reduced the amount of time it took staff to complete administrative and day-to-day tasks and has the capacity to save thousands of hours across the organisation.

In February 2025, the CPS launched 38 applications through an AI-powered low-code platform called **OutSystems**. Applications included, for example, an Advocate Panel app for private sector barristers and solicitors to apply to CPS advocate panels, and an end-to-end application for witnesses to submit expense claims. In the latter example, 64% of respondents polled in a user survey said that the time it took to get repaid was reduced from a period of several weeks to about a day.

Evidence review and analysis

Technology Assisted Review (TAR) has been in existence for at least a decade in England and Wales, and is an electronic tool which combines lawyers' subject-matter expertise with a form of AI to determine the likely relevance of documents to a particular case. As lawyers investigate and review a sample of the documents, the computer learns which documents are relevant, and which are not, and is then able to predict relevance across the entire document population. There has been judicial acceptance and encouragement of TAR (see [2016] EWHC 256 (Ch); [2016] EWHC 1464 (Ch)).

COURTS

Case management

Case management solutions, including AI transcripts, are also being explored.

> "The production of Crown Court transcripts is currently a manual process delivered by third-party suppliers. Under the contract, suppliers are required to produce transcripts to 99.5% accuracy. We are targeting a similar level of accuracy in AI transcripts. We are actively exploring opportunities to use technology to reduce the cost of transcripts in future, but a high degree of accuracy will be of paramount importance."
>
> *Secretary of State for Justice, May 2025*

'Justice AI', launched by the Ministry of Justice, piloted a **generative AI knowledge assistant** that allows court staff to ask natural language questions in order to access detailed operational procedures quickly. Current uses are administrative and operational only. The tool searches over 300 documents and returns a concise summary with source citations. Following a successful pilot, the Ministry of Justice is now exploring ways to scale the solution.

Judges in England and Wales <u>now</u> have access to **large language model AI** software on their own personal computers. The Ministry of Justice is currently **scaling AI assistants** including Microsoft Copilot, ChatGPT Enterprise and government-built alternatives across the department, following pilots across HR, policy, communications, probation and HM Courts and Tribunals Service enabling functions. The Justice AI Unit will now launch an 'AI for All' campaign, providing every Ministry of Justice staff member with secure, enterprise-grade AI assistants by December 2025.

Semantic and hybrid search tools are also in the process of being scaled across the justice system, with the aim of facilitating much improved search functionality as compared to basic keyword search.

A group of serving English judges has, however <u>emphasised</u> that whilst AI can streamline minor claims and administrative tasks, core judicial functions, such as moral reasoning, fact-finding in first-instance trials and the dignity of face-to-face justice must remain human-led.

> "[P]eople take comfort from having a human face, a human decision maker, listening to what they have to say, hearing them and making a human judgment based on the evidence. And I doubt whether AI will achieve that cathartic role that human justice does."
>
> *Judge in Focus Group 1, 2025 <u>Study</u>*

Evidence review and analysis

Oxford Institute
of Technology and Justice

Defence counsel have used AI for evidence discovery and disclosure. In 2022, a London barristers' chambers <u>used</u> **Luminance AI** to analyse over **10,000 documents** prior to a murder trial at the Old Bailey. A 20-person legal team consisting of barristers, police officers, and forensic experts was able to identify key evidence and individuals of interest, reducing the evidence review time by approximately one month, saving £50,000 in costs ahead of the trial.

"We have been served thousands of pages of evidence and material that we have to digest in a limited number of days. [...] The court digital case system has massive limitations: we're not allowed to put any unused material on there, it can't read handwritten documents, and it will only throw up the exact things you search for.

The AI learns what to search for, reads and understands and can surface in hours what would take months to find manually. The accuracy it provides is also a saving for the taxpayer"

Sally Hobson, Lead Counsel, 2020

"If you're looking through witness statements of people referencing that they saw a man with a dog and you did a keyword search for "dog" or "alsatian" that might miss the fact that someone else called it "german shepherd" or "mongrel" or "mutt". [...] Luminance is able to understand that you're looking for a man with a dog, and pull all relevant results to the lawyer. It can help find that golden nugget."

Charlotte Golunski, Senior Executive at Luminance, 2020

TRAINING

There is currently **no mandatory or systematic training** on AI for legal professionals, but the Judicial College, which provides statutory training for judges, magistrates, and others across the court system, has highlighted 'preparing for innovation and change' as a key objective in its 2023-2024 Activities Report. In July 2025, the Ministry of Justice published its *AI Action Plan*, in which it commits to supporting staff as their job roles evolve, including through training initiatives.

As part of its broader push to streamline training under its *AI Action Plan*, the Ministry of Justice in 2025 launched a **pilot initiative aimed at reducing the learning curve for its staff in using technology.** In an innovation event where small and medium-sized enterprises pitched AI-based solutions to cross-government challenges, one central focus was streamlining training for operational staff in prisons and probation services, balancing demanding on-the-job responsibilities with effective skill development. Following the event, a UK-based company was awarded a three-month contract to develop and pilot an AI-driven interactive learning platform.

The UK government has also created a new series of AI courses on 'Civil Service Learning' and provides off-the-shelf training, alongside tech firms and the Government Skills Unit.

There have also been a range of workshops, seminars and conferences for judges, prosecutors and defence counsel around the use of AI organised by, for example, LawTechUK, the Royal Society and, separately, the Ministry of Justice.

REGULATION

The UK government has set out a series of strategies, frameworks, and action plans to shape the development, regulation and application of AI across various departments. It also issued a voluntary guidance for regulators highlighting the UK's 'pro-innovation approach to AI regulation'. As at August 2025, there are no express statutory regulations governing the use of AI in criminal proceedings, or civil proceedings or court proceedings more generally. However,

several bodies have issued specific guidelines for legal practitioners, including the Courts and Tribunals Judiciary, the Bar Council, the Law Society, and the Solicitors Regulation Authority. The Crown Prosecution Service and the National Police Chiefs' Council have likewise published a set of principles to guide their adoption and use of AI. In addition, existing general laws, such as the Police and Criminal Evidence Act 1984, the Equality Act 2010, the Data Protection Act 2018, and the UK GDPR, may be construed to regulate the use of AI and AI-generated material in courts.

GUIDELINES FOR PRACTITIONERS

Judicial Office Holders

The Courts and Tribunals Judiciary for England and Wales released AI Guidance for Judicial Office Holders in December 2023, which was updatedin April 2025. The guidance distinguishes between **private AI tools and public AI chatbots**, with the latter considered less secure and less reliable. Information entered into a public AI chatbot 'should be seen as being published to all the world', according to the guidance. It clarifies that the outputs public AI chatbots provide are not 'from [an] authoritative database' and 'not necessarily the most accurate answers'. Judicial office holders are encouraged to use Microsoft's *Copilot Chat*, which is available on their devices.

The guidance encourages judges to understand AI and its applications; uphold confidentiality and privacy; ensure accountability and accuracy; be aware of biases; maintain security; take responsibility for the material produced by AI; and be aware that court/tribunal users as well as litigants may have used AI.

The guidance acknowledges that generative AI can be a 'useful secondary tool' and suggests that it **can assist with tasks such as** (1) summarising large volumes of text (without specifying the types of text concerned), (2) drafting presentations, and (3) handling administrative work (e.g. emails, transcribing and summarising meetings).

The use of generative AI is 'not recommended' for: (1) legal research, although it 'may be useful as a way to be reminded of material you would recognise as correct'; and (2) legal analysis, given that 'the current public AI chatbots do not produce convincing analysis or reasoning'.

Judicial office holders, who are 'personally responsible' for AI-generated output, are under **no obligation to document or disclose the use of AI**. The guidance likewise clarifies that '[p]rovided AI is used responsibly, there is no reason why a legal representative ought to refer to its use, [though] this is dependent upon context'. And 'until the legal profession becomes familiar with these new technologies …it may be necessary at times to remind individual lawyers of their obligations, and confirm that they have independently verified the accuracy of any research or case citations that have been generated with the assistance of an AI chatbot'.

Crown Prosecution Service

While the Crown Prosecution Service (CPS) — the prosecutorial authority in England and Wales — has no formal guidelines in place, its June 2025 mission statement entitled 'How the CPS will use Artificial Intelligence' includes a commitment to: (1) ensure 'adequate human participation in AI processes and verify the accuracy of outputs by an appropriately qualified and trained person'; (2) 'promot[e] transparency' by communicating the use of AI to all relevant parties, including suspects, and 'being transparent about the tools [they] use and how [their] data and evidence are utilised'; and (3) ensure continuous monitoring and evaluation at all stages to identify 'any unintended risk and harms'.

National Police Chiefs' Council

The National Police Chiefs' Council — a national coordination body for UK law enforcement — issued the Covenant for Using Artificial Intelligence (AI) in Policing, which was endorsed by all members of the National Police Chiefs' Council in 2023. The Covenant recognises the risks of using AI and outlines a set of principles. It states that the use of AI will be 'lawful' ('comply with applicable laws, standards, and regulations'), 'transparent' ('ensure the public are aware of AI

uses' including 'limitations of the training data'), '**explainable**' (with the 'ability … to provide an 'explanation' of its outputs' being 'a determining factor in its implementation'), '**responsible**' (with 'a human as the ultimate decision maker' where AI affects the public), '**accountable**' ('with clearly identified individuals [being] accountable for its operations and output') and '**robust**' ('with robust and reliable data' whose quality is tracked), in accordance with the College of Policing's *Code of Ethics*. It further emphasises that 'transparency and fairness must be at the heart of what we implement, to ensure a proportionate and responsible use that builds public confidence'.

> "Despite its benefits, there have been concerning examples of the use of AI in policing, where models have been built on data that led them to act disproportionately against a community or race."
>
> *National Police Chiefs' Council's* <u>*Covenant for Using AI in Policing*</u>*, 2023*

Bar Council

In January 2024, the Bar Council — the representative body for barristers in England and Wales — issued **<u>guidance</u> on the use of ChatGPT and generative AI software based on large language models** (noting that it is not 'guidance' for the purposes of the *BSB Handbook* I6.4). The Bar Council guidance acknowledges that AI adoption in legal practice is likely to increase due to technological progress and competitive pressures and states that there 'is nothing inherently improper about using reliable AI tools'. Barristers are encouraged to understand and, where appropriate, use AI tools to support their work, while maintaining control, accuracy, and compliance with professional standards.

The guidance highlights '**key risks** with LLMs', including that they are prone to hallucinations, include biases in the training data, and have the 'ability … to generate information disorder,

including misinformation'. It also notes that 'ChatGPT and other LLMs use the inputs from users' prompts to continue to develop and refine the system' and that anything entered into the system 'is used to train the software and might find itself repeated verbatim in future results', which is 'plainly problematic' if the information entered is 'confidential or subject to legal professional privilege'.

The guidance lists **'considerations' for practitioners using LLM systems**. It notes that (1) due to possible hallucinations and biases, 'it is important for barristers to **verify** the output of AI LLM software and maintain proper procedures for checking generative outputs'. Failing to do so would also be 'considered incompetent and grossly negligent' and 'may lead to disciplinary proceedings', 'professional negligence, defamation and/or data protection claims', as well as reputational damage. The guidance provides (2) that because it is difficult to understand the LLMs' internal decision-making processes ('heavy black-box' syndrome), they **'should not be a substitute for the exercise of professional judgment**, quality legal analysis and the expertise that clients, courts and society expect from barristers'. Barristers are (3) required to be **'extremely vigilant not to share with a generative LLM system any legally privileged or confidential information . . . or any personal data**, as the input information provided is likely to be used to generate future outputs and could therefore be publicly shared with others'. Such sharing would likely amount to a breach of their ethical obligations and may 'result in disciplinary proceedings and/or legal liability'. The guidance, moreover, (4) requires barristers to 'critically assess whether content generated by LLMs **might violate intellectual property rights**' and 'be careful not to use words … which may breach trademarks'. Lastly, the guidance notes that (5) it is important to **keep up to date with the 'relevant Civil Procedure Rules**, which in the future may implement rules or practice directions on the use of LLMs; for example, requiring parties to disclose when they have used generative AI in the preparation of materials'.

Law Society

In May 2025, the Law Society — the professional body for solicitors in England and Wales — issued underline guidance on the use of generative AI. It provides an overview of both the opportunities and risks the legal profession should consider when deciding whether and how to use generative AI technologies. Unlike the Bar Council's guidance, it focuses more on firm processes, risk management, client communication, governance, and also includes specific considerations for the procurement of AI tools as well as a detailed checklist of points that should be 'considered when considering generative AI use'.

The guidance highlights **key risks and steps to manage them**.

With regard to the **current generative AI regulatory landscape**, the guidance notes that there is 'no AI- or generative AI-specific regulation in the UK'. It therefore stresses the importance of understanding the capabilities and limitations of any generative AI tool intended to be used, including by assessing the provider's claims and supporting evidence. '[K]ey contractual terms of warranties, indemnities and limitations on liability' should be 'carefully negotiate[d]' with vendors and also include 'any relevant source code agreements'. The guidance further provides that there are also 'no statutory obligations on generative AI technology companies to audit their output to ensure they are factually accurate' and warns that the use of generative AI 'could result in the provision of incorrect or incomplete advice or information to clients'. It emphasises that users should '**maintain effective professional quality control over their outputs and use**', '**carefully fact-check**' and '**authenticate**' all results, and carry out '**due diligence on the AI tools in use**'. The guidance provides that although there is no legal requirement, the use of AI should be clearly communicated to clients and users should decide, in agreement with their clients, whether and how generative AI tools will be used in providing legal advice and support. If a generative AI tool does not provide an automatic usage history, users are advised to record '**all inputs, outputs, and system errors**' to enable appropriate monitoring of the tool's use.

With regard to **intellectual property**, the guidance advises to clarify in the AI vendor agreement who will hold the intellectual property rights over all input and output data, noting that some AI vendor agreements may include provisions allowing the vendor to reuse input data to refine their systems.

With regard to **data protection and privacy**, the guidance notes that 'generative AI companies may be able to see your input and output data' and that this data 'may be transferred outside UK borders' and used to train their systems. Users are therefore advised 'not [to] feed confidential information into generative AI tools, especially if [they] lack direct control and oversight' over the tool's development and deployment.

Finally, the guidance emphasises the importance of embedding **ethical principles** in the use of AI, identifying five key principles to inform the design, development, and deployment of ethical 'lawtech' (defined as '[t]echnologies that aim to support, supplement or replace traditional methods for delivering legal services or that improve the way the justice system operates') including **compliance, lawfulness, capability, transparency, and accountability**. It also notes that the UK government's principles outlined in its <u>AI white paper</u> may be useful to consider (including safety, security, and robustness; appropriate transparency and explainability; fairness; accountability and governance; and contestability and redress) as well as the <u>Public Sector Equality Duty</u> requirements which apply to AI systems used by public authorities and organisations.

In February 2022, the Solicitors Regulation Authority (SRA) – which is the independent, regulatory arm of the Law Society –released a <u>FAQ</u>highlighting compliance tips for solicitors regarding the use of AI. In November 2023, the SRA also issued a *Risk Outlook report: The use of artificial intelligence in the legal market*, which outlines how AI is used in the legal sector, its risks and how these can be overcome. The 2022 guidance notes that solicitors and firms are free 'to use any technology they think is appropriate for their business', provided it complies with the SRA's principles and standards and is underpinned by an understanding of the relevant

legal framework, particularly for AI. Senior leadership oversight is expected, with Compliance Officers for Legal Practice (COLPs) responsible for ensuring regulatory compliance when new technology is introduced, supported by board-level oversight of both procurement and ongoing use. Governance frameworks should remain fit-for-purpose to ensure responsible adoption, use, and monitoring of AI, keeping clients' best interests central. This includes leadership and oversight, risk and impact assessments, policies and procedures, training and awareness, and ongoing monitoring to avoid unintended consequences. Firms using technology platforms to deliver services must conduct due diligence to ensure compliance with obligations around confidentiality, conflicts, fee-sharing, and referral fees, and to avoid breaches such as prohibited client acquisition methods. They must offer alternatives for clients who cannot or do not wish to use legal technology. Clients should be told when they are interacting with AI, given a choice to opt out, and informed about any cost or convenience implications. Firms must make clear to clients who is responsible if technology malfunctions or causes harm, even where contracts address liability. Responsibilities should be explained at the outset, with clarity on where the client should turn for assistance.

The SRA's 2023 Risk Outlook report highlights risks associated with the use of AI, including hallucinations and biases which may lead to miscarriages of justice in criminal litigation, mislead the courts and have the potential to cause harm at a much larger scale. It also warns of highly realistic 'deepfake' images or videos used to commit crimes (scams) or submitted as evidence and addresses how risks can be managed.

Law Society of Scotland

The Law Society of Scotland issued a Guide on the Use of Generative AI in October 2024 to help solicitors understand the **key issues arising from the use of AI, in particular generative AI.** The guide highlights risks such as biases and hallucinations, as well as concerns around 'the terms of use of generative AI systems', client confidentiality, information security and data protection, and intellectual property. It emphasises that generative AI systems 'cannot replace or minimise the need for proper oversight by qualified solicitors' and that 'solicitors must recognise

that they are ultimately accountable for the advice given'. The guide warns that overreliance on AI could undermine 'the independence of solicitors', which is 'essential to the maintenance of the rule of law'. It further warns of 'systemic implications' of AI use, noting that 'wide-scale use of these systems in the domain of law necessarily increases the power of providers, including multinationals that already dominate the legal publishing market'.

Moreover, the guidance requires solicitors to ensure the system's 'explainability', meaning they should at least have 'a basic understanding' of how a generative AI system arrived at a certain result. Clients' consent to the use of AI is not required where it is used 'to assist in the provision of legal services, whether this is through automating workflow or supporting the provision of advice, such as carrying out research, summarising documents or producing draft materials'. However, if solicitors intend to input clients' 'personal data or confidential or sensitive information' related to their case into an AI system, they must not only obtain the clients' consent but ensure that additional conditions are met. These include: (1) having 'confidentiality terms in place with the provider of the generative AI system'; (2) ensuring 'security controls' are implemented; (3) ensuring the 'processing of confidential or personal data by these generative AI systems is consistent with the terms of [the solicitor's] own privacy policy and/or data protection policy'; and (4) guaranteeing that none of the data entered into the tools will be used to train the AI systems.

The guide highlights that 'personal data, client confidential or sensitive information should not be inputted into any public generative AI system'.

CRIMINAL PROCEDURE RULES

Rules governing criminal procedure establish comprehensive standards for evidence admissibility that would apply to AI-generated or AI-analysed evidence as they do to other evidence.

The **Police and Criminal Evidence Act 1984** provides courts with discretionary power to 'refuse admission of evidence which would have such an adverse effect on the fairness of the proceedings that the court ought not to admit it'. For evidence to achieve admissibility in UK criminal proceedings, it must satisfy multiple criteria: probative value (credible and adding case value), non-prejudicial character (factual and impartial), relevance (connected to case facts), coherence (logical presentation), and provability (capable of proof) (Chapter 2, Criminal Justice Act 2003).

The **Forensic Science Regulator's statutory Code of Practice** applies to AI tools used in forensic contexts. The Code, effective October 2023, applies to forensic experts in criminal proceedings and establishes quality standards for ensuring that 'accurate and reliable scientific evidence is used in criminal investigations, in criminal trials, and to minimise the risk of a quality failure'. The Code mandates validation processes demonstrating that forensic methods 'perform reliably' and requires all those undertaking forensic science activities to understand whether 'the scientific principles and methods they have relied on are valid'.

However, there is also <u>recognition</u> that 'criminal procedure must evolve to reflect the world we live in today'. In response to the Post Office Horizon scandal — a case that shocked the nation, in which hundreds of sub-postmasters were wrongly convicted based on faulty computer evidence — the UK government in 2025 launched a **call for evidence** concerning the admissibility of computer evidence, specifically, whether 'the common law presumption that a computer was operating correctly unless there is evidence to the contrary' is still fit for purpose.

DATA PROTECTION LEGISLATION

Existing data protection legislation may also regulate the use of AI in criminal proceedings.

The *Data Protection Act 2018 and UK GDPR* contain specific provisions governing automated decision-making. Under the existing framework, there is a general prohibition on automated decision-making for law enforcement purposes, except where certain, limited, conditions apply.

The Data (Use and Access) Act 2025 amends those provisions to open up the range of lawful bases *permitting* the processing of personal data for automated decision-making purposes, which would apply to AI systems. Following the amendments made by the Data (Use and Access) Act 2025, which is anticipated to come into force within the next 12 months, an automated decision is one in which 'there is no meaningful human involvement in the taking of the decision'. Generally, the Act eases the constraints on organisations using automated decision-making systems, although stringent requirements remain for 'significant decisions'—i.e. those that 'produce an adverse legal effect for the data subject, or have a similarly significant adverse effect for the data subject' (s 80(3), Data (Use and Access) Act 2025). Organisations processing personal data for the purpose of automated decision-making are permitted to rely on **'legitimate interests' as a lawful basis for such processing which for example include crime prevention, detection and investigation as well as national security, public security and defence purposes.** This is provided that the organisation ensures that suitable safeguards are in place. These include providing individuals with detailed information about the use of automated decision-making, including the decision-making logic and the data used, offering the right to request a human review, conducting impact assessments to evaluate risks and benefits, and implementing accountability measures, such as regular audits and compliance checks. However, **'significant decisions' require** organisations to have one of the following legal bases to justify automated decision-making: **explicit consent, necessity for contract performance, or a substantial public interest justification.** More restrictive provisions also apply to significant decisions involving special category personal data (such as health data, racial or ethnic origin, political beliefs, religious views), or biometric and genetic information used for unique identification.

HUMAN RIGHTS

The *Human Rights Act 1998* and *the Equality Act 2010* may also constrain the use and deployment of AI.

The **Human Rights Act 1998**, incorporating Article 6 of the European Convention on Human Rights, guarantees fair trial rights. Article 6 ensures 'a fair and public hearing within a reasonable

time by an independent and impartial tribunal established by law' and applies to criminal as well as civil proceedings.

The **Equality Act 2010** requires all public bodies to consider how their activities, including algorithmic decision-making, impact inequality. Public authorities must 'eliminate discrimination, harassment, victimisation', 'advance equality of opportunity', and 'foster good relations between persons who share a relevant protected characteristic and persons who do not share it' (s 149, *Equality Act 2010*). The Court of Appeal's decision in *R (Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058 demonstrates the practical application of that broad duty to the deployment of automated technology, finding that police failed to adequately consider the discriminatory impacts of facial recognition technology.

International frameworks may also provide guidance. The UK is a member of the Council of Europe. In September 2024, the UK signed the Council of Europe's *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*. The Convention covers the use of AI in the public sector, aiming to ensure compliance with human rights and highlighting fundamental principles such as human dignity, equality and non-discrimination, privacy and personal data protection, transparency and oversight, accountability and responsibility, as well as reliability. Previously, in December 2018, the Council of Europe, had adopted the first European Ethical Charter on the use of artificial intelligence in judicial systems (the 'Ethical Charter'). The Ethical Charter provides for certain core principles to be respected in the field of AI and justice, including respect of fundamental rights, non-discrimination, transparency, and 'user control'. The UK has, however, not taken any specific steps to implement the Ethical Charter. Relevant guarantees, including the right to a fair trial and privacy rights, under other international human rights treaties to which the UK is a party, such as articles 14 and 17 of the *International Covenant on Civil and Political Rights* or articles 16 and 40 of the Convention on the Rights of the Child, may also be relevant.

OUTLOOK

In July 2025, the Ministry of Justice (MoJ) published the **AI Action Plan for Justice**, outlining its approach to **transforming the justice system** in England and Wales, including by 'embedding AI across the justice system'. The MoJ Plan emphasises the importance of 'strengthening […] foundations' by 'enhanc[ing] AI leadership, governance, ethics, data, digital infrastructure and commercial frameworks'. In its AI rollout it also plans to focus on 'high-impact use cases', including: (1) reducing the administrative burden through secure efficiency-related AI tools; (2) improving access to justice via citizen-facing assistants; (3) supporting better decision-making through predictive and risk-assessment models (non-generative AI); and (4) personalised education and rehabilitation through AI.

It will launch an **'AI for All' campaign,** which aims to provide 'every MoJ staff member with secure, enterprise-grade AI assistants by December 2025, accompanied by tailored training and support'. These tools are intended to help staff work more efficiently, collaborate more effectively, and focus on tasks that should be done by humans.

The Plan emphasises that AI should enhance, rather than replace, human skill, talent, and judgment. As a result, the Plan seeks to 'invest in […] people and partners' by recognizing that AI adoption often fails not only due to 'technological limitations, but because people and processes are not supported to adopt'. To address this, the MoJ will work closely with the Director General for People and Capability and trade unions to support staff as their roles evolve. This will include training initiatives, proactive job redesign, and incentives that promote a people-centred approach to technology adoption.

CASES

In September 2025, in the First-tier (Tax) Tribunal, the Tribunal Judge confirmed that he used Microsoft Copilot to assist in producing his decision. This is the **first reported case in England and Wales confirming the use of AI by a judge.** In *VP Evans v The Commissioners for His Majesty's Revenue and Customs* [2025] UKFTT 1112 (TC), Tribunal Judge McNall explained that he used Microsoft Copilot (through the private eJudiciary platform) to summarise documents

submitted by the parties, treating these summaries only as a first draft and personally verifying their accuracy, while emphasising that he did not use AI for legal research and that the evaluative judgment and weighing of arguments remained entirely his own. Judge McNall stated that the case was particularly well-suited to this approach as it was a discrete case management matter decided on the papers without a hearing or credibility determinations, and that, unlike public large language models, Copilot maintains data security and privacy protections when judicial office holders are logged into their eJudiciary accounts.

In a series of cases, English courts have addressed the misuse of AI by legal professionals and litigants in proceedings, so far in non-criminal cases, and examined the lawfulness of emerging technology.

Facial Recognition

In *R (Bridges) v Chief Constable of South Wales Police [2020] EWCA Civ 1058,* the Court of Appeal ruled that the use of automated facial recognition technology by the South Wales Police was unlawful and violated Article 8 of the *European Convention on Human Rights*, which protects the right to respect for private and family life, as well as the *Data Protection Act 2018*and the Equality Act 2010. The Court found that there was insufficient guidance on the use of the automated facial recognition technology and that South Wales Police had failed to take reasonable steps to ensure the technology did not exhibit gender or racial biases, stating that this 'is a novel and controversial technology [and that] all police forces that intend to use it in the future would wish to satisfy themselves that everything reasonable which could be done had been done in order to make sure that the software used does not have a racial or gender bias'. However, the Court did not categorically prohibit the use of such technology, acknowledging that its potential benefits could outweigh the human rights concerns. Nonetheless, the ruling deemed the use of the technology in that case unlawful due to the absence of a proper legal basis, inadequate impact assessments, and insufficient safeguards.

Electronic Disclosure

Certain forms of AI are being increasingly used in the context of electronic disclosure. Technology-Assisted Review (TAR), or predictive coding, was endorsed in civil proceedings in *Pyrrho Investments Ltd v MWB Property Ltd* [2016] EWHC 256 (Ch). In its ruling, the Court described this as a tool where 'review of the documents concerned is being undertaken by proprietary computer software rather than human beings. The software analyses documents and 'scores' them for relevance to the issues in the case'. While the Court was keen to note that use of such software will depend on the particular circumstances of each case, **the Court endorsed its use in the context of proceedings where traditional 'manual' review of what amounted to over 3 million documents would result in unreasonable costs.** More recent procedural guidance in the business and property courts now anticipate that parties will actively consider technology or computer assisted review software as part of conducting disclosure of electronic documents.

Misuse of AI in Court Filings

Courts have addressed the use or suspected misuse of AI by legal professionals in proceedings in non-criminal cases.

For example, in its June 2025 judgment related to duties owed by lawyers in the court in *Ayinde v London Borough of Haringey and Al-Haroun v Qatar National Bank [2025] EWHC 1383 (Admin),* the High Court issued a stark warning to lawyers for citing non-existent case law, stating that '[w]here [lawyers'] duties are not complied with, the court's powers include public admonition of the lawyer, the imposition of a costs order, the imposition of a wasted costs order, striking out a case, referral to a regulator, the initiation of contempt proceedings, and referral to the police'. 'Placing false material before the court with the intention that the court treats it as genuine may, depending on the person's state of knowledge, amount to a contempt … because it deliberately interferes with the administration of justice', the Court observed. It added that 'proceedings for contempt of court may be initiated … by the court of its own motion … or by anyone with a sufficient interest'. The Court also urged legal regulators to address the misuse of AI.

In its ruling, the Court recognised that **AI 'is a powerful technology [and] can be a useful tool in litigation, both civil and criminal'. Given the risks it carries, '[i]ts use must take place therefore with an appropriate degree of oversight, and within a regulatory framework that ensures compliance with well-established professional and ethical standards if public confidence in the administration of justice is to be maintained'. The Court added that 'the administration of justice depends upon the court being able to rely without question on the integrity of those who appear before it and on their professionalism in only making submissions which can properly be supported'.** The ruling referred to solicitors' and barristers' regulatory duties and cited the Bar Council's published guidance *Considerations when using ChatGPT and generative artificial intelligence software based on large language models* as well as the Solicitors Regulation Authority's *Risk Outlook report*. It also observed that 'there is no shortage of professional guidance available about the limitations of artificial intelligence and the risks of using it for legal research' and expressed 'concerns about the competence and conduct of the individual lawyers who have been referred to this court . . . as well as broader areas of concern … as to the adequacy of the training, supervision and regulation of those who practise before the courts' as well as 'the practical steps taken by those with responsibilities in those areas to ensure that lawyers who conduct litigation understand and comply with their professional and ethical responsibilities and their duties to the court'.

The two cases (Ayinde v London Borough of Haringey and Al-Haroun v Qatar National Bank [2025] EWHC 1383 (Admin)), were referred to a Divisional Court of the King's Bench Division of the High Court for review and enforcement of the lawyers' duties owed to the court, addressing serious professional misconduct after the suspected use of generative AI.

In *Ayinde v London Borough of Haringey*, the claimant's legal team cited five fake authorities when arguing the grounds for judicial review against the London Borough of Haringey for its failure to provide interim accommodation pending a homelessness review. The defendant's solicitor applied for a wasted costs order against the claimant's legal team on the basis that they had relied on fabricated cases. The judge determining the wasted costs order found that, by

submitting fake authorities, the barrister and solicitors had acted 'improperly, unreasonably and negligently', and ordered them to pay £2,000 to the defendant. The case was then referred to the High Court, which has jurisdiction over lawyers' compliance with court procedures and duties owed to the court (the so-called *Hamid* jurisdiction). While the High Court did not initiate contempt proceedings, the matter was referred to the Bar Standards Board and the Solicitors Regulation Authority.

In *Al-Haroun v Qatar National Bank*, in which the claimant sought damages of £89.4 million against the Qatar National Bank and alleged breach of a financing agreement, the claimant's solicitor submitted witness statements referencing 18 authorities that were either fictitious or inaccurately cited. The case was also referred to the Divisional Court, and listed with *Ayinde*, for review under the court's *Hamid* jurisdiction. The claimant admitted that he had drafted the materials using AI which his lawyer did not verify. The Court found no intent to mislead but given the 'lamentable failure to comply with the basic requirement to check the accuracy of materials before the court', it referred the solicitor to the Solicitors Regulation Authority.

> "There are serious implications for the administration of justice and public confidence in the justice system if artificial intelligence is misused. In those circumstances, practical and effective measures must now be taken by those within the legal profession with individual leadership responsibilities (such as heads of chambers and managing partners) and by those with the responsibility for regulating the provision of legal services … [P]romulgating [...] guidance on its own is insufficient to address the misuse of artificial intelligence. More needs to be done to ensure that the guidance is followed and lawyers comply with their duties to the court. … We invite [the Bar Council and the Law Society, and the Council of the Inns of Court] to consider as a matter of urgency what further steps they should now take in the light of this judgment."
>
> *Dame Victoria Sharp, President of the King's Bench Division, June 2025* ruling

In *Bandla v Solicitors Regulation Authority [2025] EWHC 1167,* the solicitor seeking to appeal against the decision by the SRA to strike him off the roll (in relation to other unrelated conduct) submitted, in materials put before the Court in connection with the appeal, a number of non-existent authorities. The Court <u>stated</u> that it needed to **'take decisive action to protect the integrity of its processes against any citation of fake authority' and accordingly struck out the grounds of appeal submitted as an abuse of process.** The Court awarded indemnity costs against the appellant on that basis.

Similarly, courts have addressed the misuse of AI by unrepresented litigants in non-criminal cases.

In *Harber v The Commissioners for His Majesty's Revenue and Customs [2023] UKFTT 1007 (TC),* the Court <u>noted</u> that 'citing invented judgments […] causes the Tribunal and HMRC **to waste time and public money,** and this reduces the resources available to progress the cases of other court users who are waiting for their appeals to be determined'.

In *Olsen v Finansiel Stabilitet A/S* [2025] *EWHC 42 (KB)*, the Court <u>warned</u>that the submission of false or inauthentic materials to the Court can give rise to a risk of **contempt proceedings as well as adverse costs orders.**

In *Zzaman v The Commissioners for His Majesty's Revenue and* Customs [2025] *UKFTT 539 (TC)*, the Court <u>advised</u> litigants to carefully check AI-generated output and **offered practical advice**, noting that 'dangers can be reduced by the use of clear prompts, asking the tool to cite specific paragraphs of authorities (so that it is easy to check if the paragraphs support the argument advanced), checking to see the tool has access to live internet data, asking the tool not to provide an answer if it is not sure and asking the tool for information on the shortcomings of the case being advanced'.