COLLAS CRILL

Generative AI and legal privilege: What boards need to know

APRIL 2026

Generative AI is already part of how many organisations work, and staff will increasingly turn to it to assist with their work, even in businesses that have not officially addressed its use.

Directors are being asked to balance the gains associated with generative AI against legal and regulatory risk.

One area that presents particular challenges is legal professional privilege. If privilege is inadvertently lost then sensitive material may need to be disclosed to opponents in the event of litigation.

This article considers potential risks in this evolving area of law. Although it does not consider the law of any specific jurisdiction, the types of privilege discussed in this article are based on the law of England and Wales. They will be relevant to many commonwealth jurisdictions, including those in which Collas Crill operates.

Key takeaways

- **The law is not settled**: using generative AI in a legal context carries real (and evolving) privilege risks.
- **Data security matters**: you must understand how your generative AI tools handle, store and use data.
- **Uncontrolled use can undermine privilege**: even with secure tools, policy and oversight must be deployed carefully to control how generative AI is used.

What is legal professional privilege?

Privilege protects certain communications from disclosure. Two main types are relevant when considering generative AI:

1. Legal advice privilege

Legal advice privilege applies to confidential communications between a client and a lawyer for the purpose of giving or receiving legal advice. It allows parties to communicate openly with their legal advisors without having to worry about subsequent disclosure.

Legal advice privilege is typically limited to communications with a lawyer. It does not extend to general internal discussions or advice from non-lawyers.

2. Litigation privilege

This note is a summary of the subject and is provided for information only. It does not purport to give specific legal advice, and before acting, further advice should always be sought. Whilst every care has been taken in producing this note neither the author nor Collas Crill shall be liable for any errors, misprint or misinterpretation of any of the matters set out in it. All copyright in this material belongs to Collas Crill.

This can apply more broadly, including communication with third parties, but only where:

- litigation is in reasonable contemplation, and
- the document is created for the dominant purpose of conducting that litigation.

A critical feature of both legal advice privilege and litigation privilege is confidentiality. If the confidentiality of a document is lost then privilege may be lost with it.

Where generative AI creates risk

If you don't take care over selecting the generative AI tools being used in your business and how they are being used, you risk losing privilege in two ways.

Loss of privilege via loss of confidentiality

If privileged material is shared with a third party in circumstances where confidentiality is not preserved, privilege may be waived.

This could take place by inputting the material into a generative AI tool, or inviting an AI notetaker to a meeting at which privileged material is discussed.

The risk was highlighted in *Munir v Secretary of State for the Home Department* [2026] UKUT 81, an English case in which a solicitor had been entering client data into an insecure generative AI tool:

'Uploading confidential documents into an open-source AI tool, such as ChatGPT, is to place this information on the internet in the public domain, and thus to breach client confidentiality and waive legal privilege...'

Although this comment was an aside and doesn't give rise to any new legal principle, it illustrates how privilege could be unwittingly lost by way of a loss of confidentiality.

In order to ensure that confidentiality is not lost over data input into a generative AI tool, you should ensure that:

- the contract with the provider contains adequate confidentiality provisions; and
- your data cannot be used to further train an AI model.

Beware vague marketing labels like 'closed' and 'enterprise', which may not accurately reflect the confidentiality provisions within the supplier's terms.

No privilege for legal questions to generative AI

Crucially, there is another way that generative AI use can lead to you losing privilege over key data (or, more accurately, never benefitting from privilege in the first place).

Legal advice privilege applies only to communications with a lawyer, so prompts to, and outputs from, generative AI tools are unlikely to be privileged.

This creates a subtle but important risk. If employees use generative AI to explore legal issues rather than asking a lawyer, then that data will often not be privileged, even if the tool maintains confidentiality.

If a dispute later arises, those records could be disclosable to the other side, potentially revealing:

- internal thinking;
- early risk assessments; or
- inconsistencies in position.

Litigation privilege may still apply in circumstances where litigation is already in reasonable contemplation, but routine or exploratory use of AI on legal topics like this will often fall outside that scope.

It should also be noted that generative AI is not a reliable source of legal information, due to:

- its tendency to hallucinate (ie give convincing but inaccurate responses); and
- the typical lack of contractual accountability for these inaccuracies in AI suppliers' terms.

What should boards be doing?

Boards should be taking practical steps to address the risks to privilege presented by generative AI.

1. Ensure frameworks consider privilege risk alongside other data risks

Privilege risk should be considered alongside other data risks in governance frameworks.

2. Focus on real data safeguards

As with other data risks, analysis needs to look beyond a tool's branding to assess:

- contractual protections regarding data use; and
- actual technological controls.

3. Control how staff use AI tools

Policies and training are critical. In particular:

- prohibiting the input of sensitive material into unapproved tools, or prohibiting the use of such tools altogether;
- defining what issues should be escalated to lawyers instead of being entered into generative AI tools; and

- similarly regulating the use of AI notetaking.

Final thought

Generative AI can deliver real efficiency gains and improve the client experience, but improperly regulated use can give rise to an obligation to disclose damaging documents, which you otherwise could have protected with privilege.

If you would like to discuss how to best maintain privilege in your organisation in the face of rapidly evolving technology, please get in touch with our team.

This note is a summary of the subject and is provided for information only. It does not purport to give specific legal advice, and before acting, further advice should always be sought. Whilst every care has been taken in producing this note neither the author nor Collas Crill shall be liable for any errors, misprint or misinterpretation of any of the matters set out in it. All copyright in this material belongs to Collas Crill.

COLLAS CRILL

For more information please contact:

Jack Crisp

Professional Support Lawyer | Guernsey

t: +44 (0) 1481 734837 | **e:** jack.crisp@collascrill.com

Gareth Bell

Guernsey Managing Partner | Guernsey

t: +44 (0) 1481 734214 | **e:** gareth.bell@collascrill.com

Rocco Cecere

Partner | Cayman

t: +1 345 914 9630 | **e:** rocco.cecere@collascrill.com

Nuno Santos-Costa

Partner | Jersey

t: +44 (0) 1534 601731 | **e:** nuno.santoscosta@collascrill.com

Stuart Cullen

Partner | BVI

t: +1 284 852 6310 | **e:** stuart.cullen@collascrill.com

Lilla Zuill

Managing Partner | Bermuda

t: +1 441 405 1500 | **e:** lilla.zuill@collascrill.com

This note is a summary of the subject and is provided for information only. It does not purport to give specific legal advice, and before acting, further advice should always be sought. Whilst every care has been taken in producing this note neither the author nor Collas Crill shall be liable for any errors, misprint or misinterpretation of any of the matters set out in it.