

June 3, 2026

LEGAL ALERT

Every Chat Is Evidence: The Hidden Discovery Risk in Your Organization's Use of Generative AI

Recent federal decisions confirm that a client's conversations with artificial intelligence tools, including ChatGPT, Claude, Gemini, and Copilot, are generally discoverable in litigation and are not protected by the attorney-client privilege. Board members, administrators, and staff who use these tools to draft, brainstorm, or analyze sensitive matters should assume that every word typed into the chat box may one day be produced to opposing counsel, a regulator, an investigator, or a journalist in response to a public records request.

The most consequential ruling to date is United States v. Heppner, (S.D.N.Y. Feb. 2026), in which the court held that communications with Anthropic's Claude were not shielded by the attorney-client privilege, even after they were forwarded to counsel, because 1) the defendant's engagement with Claude was not a communication between himself and his attorney, 2) the defendant's communications with a third-party AI platform were not confidential, and 3) the defendant did not communicate with Claude for the purpose of obtaining legal advice because Claude itself disclaims providing legal advice and the defendant consulted it on his own initiative rather than at his attorney's direction. The court also held that the documents the defendant generated using Claude were not shielded by the work-product doctrine because he created them on his own initiative rather than at counsel's direction and therefore did not reflect his attorney's strategy at the time they were created, even if those documents affected his attorney's strategy afterward. While Heppner is persuasive rather than binding in California courts, it is consistent with at least one California ruling and another New York ruling.

©2026 LAW OFFICES OF YOUNG, MINNEY & CORR, LLP

Public Agency Exposure

For public agencies, including charter schools, the risk of exposure of records is significant. Drafting sensitive documents in a consumer chatbot – such as employee discipline memoranda, constituent or parent communications, intake summaries for harassment complaints, special education correspondence, or internal investigation notes, among other things -- can create a written record that is recoverable through discovery and, in many cases, may be responsive to a California Public Records Act (CPRA) request. The CPRA reaches writings prepared, owned, used, or retained in the conduct of the public's business, regardless of the device on which it was created. See City of San José v. Superior Court, 2 Cal.5th 608, 619 (2017). So, if an administrator uses ChatGPT on their personal phone to work through a staff issue, that conversation can still be requested by the public and pulled into a lawsuit – even though it never ran through an agency computer or email account.

In addition, consumer AI tools' standard terms of service generally permit the vendor to use submitted content for model training and to allow human review for safety and quality control, and, as was the case in Heppner, may be disclosed to a host of third parties, including governmental regulatory authorities. This means that submitting personnel records, student records, or employee health information to a free or standard tool may independently breach the organization's privacy commitments and California's broader privacy framework, including, where applicable, the Student Online Personal Information Protection Act at Business and Professions Code section 22584.

Private Organization Exposure

Private schools, nonprofits, and other private organizations are not subject to the CPRA, but discovery exposure remains. Administrators, directors, business officers, board members who use consumer AI to draft termination memoranda, discipline letters, or responses to parent complaints, for example, create discoverable records of their reasoning and word choices that opposing counsel can and will demand in subsequent litigation.

Recommended Steps

Organizations should treat generative AI the way they treat email and text messaging: as a recoverable, discoverable medium that must be governed by written policy, training, and records-management protocols.

In the near term, organizations should:

1. Adopt or update an AI-use policy covering board members, administrators, and staff;

©2026 LAW OFFICES OF YOUNG, MINNEY & CORR, LLP

2. Require enterprise-grade tools with contractual no training and zero data retention policies for any matter involving personnel, student records, confidential information, civil rights complaints, or anything involving or likely to lead to litigation. If a matter is already in litigation or under investigation, counsel should be consulted before using any AI tool to analyze or draft documents bearing on the dispute;
3. Update existing litigation hold notices and retention schedules to expressly include AI chat histories, exports, and prompt logs; and
4. Refresh training for boards and staff to address AI risks and the proper use of AI.

###

Young, Minney & Corr LLP is available to assist with policy drafting, vendor contract review, litigation hold updates, and board and administrator training; please contact Paul Minney (pminney@ymclegal.com) or Kaela Haydu (khaydu@ymclegal.com) to discuss the application to your organization's circumstances.

Young, Minney & Corr, LLP's Legal Alerts provide general information about events of current legal importance; they do not constitute legal advice. As the information contained here is necessarily general, its application to a particular set of facts and circumstances may vary. We do not recommend that you act on this information without consulting legal counsel.

©2026 LAW OFFICES OF YOUNG, MINNEY & CORR, LLP