

THIRD PARTY AI TOOL USAGE

PURPOSE

This policy establishes guidelines for the appropriate use of third-party AI tool usages by Centric Consulting, LLC's ("Centric" or "Centric Consulting") associates in the workplace. This policy aims to ensure that AI tools are used consistent with Centric Consulting's values, ethical standards, and legal obligations. While this policy applies broadly to all AI tool usage, certain uses, particularly those involving employment-related decisions, client information, personal data, or other sensitive or confidential information, carry heightened legal, ethical, and compliance risks and therefore require additional care and adherence to the requirements set forth in this policy. Examples of AI tools covered by this policy include but are not limited to:

- Content Generation (e.g., Copy.ai, OpenAI ChatGPT and associated models, Jasper)
- Image Generation Services (e.g., MidJourney, StableDiffusion, OpenAI's Dall-E)
- PowerPoint Tools (e.g., Beautiful.ai)
- Note Taking and Transcription (Mem, Otter)
- Automation (Zapier)
- Text Enhancement (Grammarly, Wordtune)

SCOPE

For the purposes of this policy the term "associates" refers to all employees, contractors, consultants, temporary employees, and all other workers at Centric, including all personnel affiliated with third parties. This policy applies to all associates who use AI tools in their work. It covers the use of AI tools on company-owned devices, as well as personal devices used for work purposes.

This policy applies to all subcontractors and third-party personnel performing work on behalf of Centric, regardless of whether such individuals work on Company-owned or personal devices. Centric will incorporate appropriate AI use requirements into its statements of work, master service agreements, and subcontractor agreements to ensure that all third parties engaged by Centric Consulting comply with this policy. Associates responsible for contracting with subcontractors or third parties should consult with Centric Legal to confirm that appropriate contractual provisions are in place.

POLICY

AUTHORIZED USE:

Centric has designated Microsoft as its default AI platform for internal productivity, solution development, and scalable AI delivery. Associates should use approved Microsoft-based AI tools, including Microsoft Copilot, Microsoft 365 Copilot, Copilot for Sales, and GitHub Copilot,

when those tools reasonably satisfy the business need. If there is a business need to use a non-Microsoft AI tool, the use must be supported by a clear business rationale and approved by the applicable NVP. If a client has a preference for an AI platform that differs from Microsoft, associates should use the preferred tool in the client's environment for that work, provided the use is consistent with applicable client agreements, client policies, and this policy (including but not limited to all confidentiality restrictions). Subject to these requirements, associates are authorized to use AI tools to support their work-related tasks, including but not limited to research, drafting documents, generating content, and answering questions. Associates must use AI tools consistent with Centric Consulting's Code of Conduct and other applicable policies, including any applicable client policies.

Notwithstanding the authorized uses described above, associates may not use AI tools for the following purposes:

- To make or significantly drive any employment decision, including hiring, promotion, demotion, discipline, or termination, without independent human review and validation of the AI-generated output.
- To impersonate any individual, create false identities, or generate documents, communications, images, audio, video, or other content that is fraudulent, false, or misleading.
- To process, analyze, or generate content related to any matter for which the associate has a conflict of interest without prior disclosure to and approval from Centric Legal.
- To circumvent or attempt to circumvent any security control, data loss prevention tool, or access restriction implemented by Centric IT.
- To access, process, or transmit any information in violation of applicable law, including but not limited to applicable privacy laws, export control laws, and consumer protection laws.

ETHICAL AND LEGAL CONSIDERATIONS:

Associates must use AI tools in an ethical and lawful manner. This includes, but is not limited to, the following:

- Respecting intellectual property rights and not using AI tools to generate or distribute copyrighted or plagiarized content.
- Refraining from use of AI tools to create or disseminate false, misleading, or defamatory information.
- Refraining from use of AI tools to engage in discriminatory, harassing, or offensive behavior.

- Complying with all applicable federal, state, and local employment laws when using AI tools in connection with human resources, including but not limited to Title VII of the Civil Rights Act, the Americans with Disabilities Act, the Age Discrimination in Employment Act, the Fair Credit Reporting Act, applicable state biometric privacy laws, and any jurisdiction-specific automated employment decision tool laws. Associates should consult Centric Legal if they are uncertain whether a particular AI use in an employment context complies with applicable law.
- Disclosing the use of AI tools to clients or other recipients of work product when required by applicable law, applicable client policies, or applicable professional standards, or when the client has specifically requested such disclosure. Associates should consult Centric Legal if they are uncertain whether disclosure is required in a particular engagement.

CONFIDENTIALITY AND DATA SECURITY:

Associates must exercise caution when using AI tools to avoid accidental or intentional exposure of sensitive or confidential information. Centric IT and Centric Legal have analyzed different AI tools and certain tools have been approved for handling confidential, proprietary, or personally identifiable information. These tools (“Centric AI Approved Tools” or “CAATs”) are listed on Schedule A, which may be updated from time to time. If the Associate is using a CAAT, the Associate may send confidential information to the CAAT, but only with specific written authorization from the client acknowledging that their data will be processed within Centric’s infrastructure which may not provide sufficient levels of data protection in comparison to other, previously signed agreements with the client. The CAAT designation indicates that a tool has been reviewed for appropriate handling of confidential information within the CAAT itself; it does not override the need for approval from the client in regards to the use or storage of client information on Centric’s networks and any client data used or stored on Centric’s network should only be used for the specific CAAT interaction / processing and then deleted.

If the Associate is not using a CAAT, Associates should do so with an expectation that it is not protected by the platform and as such should limit the types of data that they send and should not include any confidential information of Centric or of Centric’s previous, active, or prospective clients. Therefore, associates should not input or share any client-specific, proprietary, or confidential information with AI tools unless the platform is considered a CAAT.

If the platform is not considered a CAAT:

- Do not send client information to any non-CAAT AI tools without written approval from both Centric Legal and the Client.

- Do not send Centric proprietary or confidential information to any non-CAAT AI tools including but not limited to trade secrets, financial information, account contact information, employee specific information without consent, or legal documents to which Centric is a party. For example, while ChatGPT can take a SOW (Statement of Work) and create a case study, SOWs contain confidential Centric and client information in them, so associates should not paste SOWs into ChatGPT.
- Do not send any identifiable information to any non-CAAT AI tools including but not limited to: Personally Identifiable Information (PII) and Protected Health Information (PHI).
- Do not send candidate application data, interview recordings, interview transcripts, or summaries of interviews to any non-CAAT AI tool. Do not send employee performance data, personnel file contents, compensation information, or disciplinary records to any non-CAAT AI tool.

AI TOOL ACCESS, PERMISSIONS, AND AUTOMATED CAPABILITIES:

In addition to considering the information shared with AI tools, associates must carefully evaluate the access, permissions, and capabilities granted to those tools. Many AI tools can access files, integrate with other systems, operate continuously, or take actions on a user's behalf. Improper configuration or excessive permissions may result in unauthorized data access, unintended actions, or violations of Company security controls.

Associates must apply the principle of least privilege when enabling or configuring any AI tool and may only grant the minimum access required for the approved business purpose.

Unless a tool is a Centric AI Approved Tool (CAAT) and explicitly approved for the intended use, associates may not:

- Grant AI tools access to local devices, file systems, email, browsers, collaboration tools, or other Company systems.
- Allow AI tools to operate autonomously, continuously, or in the background.
- Use AI tools to take actions on Company or client data without active human review.
- Share company credentials or authentication artifacts with the AI tool, including usernames, passwords, multi-factor authentication codes, API keys, access tokens, or certificates, or allow the tool to "log in as the associate" or act on the associate's behalf.

For purposes of this policy, use of an AI tool includes installing, enabling, configuring, authorizing integrations, or granting permissions, even if the tool has not yet been actively

used. Associates who are uncertain whether a tool's access or capabilities comply with this policy must consult Centric IT or Centric Legal before use.

AI Use in Human Resources (Talent Acquisition, Total Rewards, Talent Management, and Performance Management):

The use of AI tools in human resources contexts, including but not limited to candidate interviews, applicant screening, employee performance reviews, and related employment activities presents heightened legal, ethical, and compliance risks. Accordingly, associates involved in these functions must comply with additional requirements and safeguards set forth in this section.

Associates may use AI tools for administrative efficiency purposes, such as transcription, summarization, drafting, compiling information, and organizing documentation. Associates may not use AI tools to score, rank, or recommend candidates or employees, generate final performance ratings, make disciplinary determinations, or otherwise produce outputs that inform or drive employment decisions without meaningful human review and validation of those outputs. Managers and supervisors bear full responsibility for the accuracy, fairness, and legal compliance of all final evaluations and employment decisions, regardless of whether AI tools assisted in the process.

AI tools used in Human Resources functions must not screen out protected groups, draw inferences related to disability or other protected characteristics, or produce results that have a disparate impact on any protected class under applicable federal, state, or local law. Associates must review AI-generated outputs for potential bias before using those outputs in any capacity related to hiring, evaluation, or other employment decisions.

Associates must not input candidate personally identifiable information, personally identifiable employee information, protected health information, or confidential personnel data into any non-CAAT AI tool. Candidate and employee data, including interview recordings, transcripts, summaries, performance data, compensation information and personnel documentation, must be stored only on Company-designated platforms and must not be shared externally except as required by applicable law. Any AI-generated content used in connection with a performance review, hiring, or disciplinary matter must be reviewed and validated by the responsible manager or decision-maker before it is included in any official record or communicated to the candidate or employee.

Centric Consulting records interviews and transcribes using AI tools only with the express written consent of the candidate, consistent with applicable multi-state recording laws. Written consent is obtained as part of the application process. Talent Acquisition is responsible for confirming that the required consent and any applicable jurisdiction-specific notices have been provided before any interview is recorded. For candidate awareness, the interview confirmation will disclose that the interview may be recorded. At the outset of any interview that will be recorded, the interviewer must verbally notify the candidate that the interview will be recorded and obtain the candidate's verbal acknowledgment before starting the recording.

Centric Consulting prohibits candidates from recording interviews or using AI tools during interviews, consistent with the disclosures and restrictions set forth in Centric Consulting's external application materials. Associates who become aware of a candidate recording an interview or using AI tools during an interview should document the conduct and consult with Centric Legal before taking further action.

Associates must report any AI tool used in a Human Resources context that has not been previously reviewed and approved by Centric IT and Centric Legal to CentricIT@centricconsulting.com before using that tool.

Centric will not use AI tools to make or substantively drive any employment decision, including hiring, termination, demotion, or disciplinary action, without a human decision-maker conducting an independent review of the basis for that decision.

BRAND REPRESENTATION AND EXTERNAL USE:

Centric's brand is a shared business asset that carries the trust and reputation that lead clients to choose us. AI can help associates create client-facing materials more quickly, but it also increases the risk that materials bearing Centric's name may be shared externally without appropriate review.

Whenever AI tools are used to create, edit, or assist with material that is published, distributed, or presented externally under Centric's name, brand, or identity, they must ensure the material is consistent with Centric's approved brand standards. This requirement applies to websites and landing pages, documents and presentations, proposals and pitch materials, social media, emails, any client-facing deliverable, and internal material that is likely to become external. Associates must take care of how they represent Centric's brand and as such must not:

- Use AI tools to create, modify, recreate, approximate, or extend Centric’s official brand identity, including logos, wordmark, taglines, slogans, sub-brands, visual identities, or co-branded lockups without approval from National Marketing
- Use AI-generated images, illustrations, or video in a manner inconsistent with Centric's approved brand standards. Media assets should be sourced from approved libraries wherever possible rather than generated.

AI TOOL VETTING AND APPROVAL:

Centric Consulting maintains a curated set of Centric Approved AI Tools (“CAATs”) that have been reviewed by Centric IT and Centric Legal for data security, privacy, and confidentiality purposes. Before any AI tool that is not currently listed on Schedule A as a CAAT may be used to process confidential, proprietary, or personally identifiable information, the tool must be submitted for review. Prior to requesting review of a new AI tool, associates must evaluate whether the intended use case can reasonably be satisfied using an existing CAAT or other approved company technology. To request review of a new AI tool, an OG lead must email CentricIT@centricconsulting.com with the following information:

1. Tool name and vendor information.
2. Intended use case.
3. Business justification detailing the reasons why current CAATs are unable to fulfill the identified requirements.
4. Available terms of service or data processing documentation for the tool.

Associates may not use a non-CAAT tool to process confidential, proprietary, or personally identifiable information until the tool is reviewed and approved.

Centric IT and Centric Legal will review submitted tools on a reasonable and timely basis. The review will assess, at minimum, the vendor's data security and privacy practices, the tool's data retention and training practices, the tool's terms of service and any applicable data processing agreement, and the potential legal and reputational risk associated with the tool's use.

Tools approved through this process will be added to Schedule A. Tools that do not meet Centric Consulting's standards will not be approved, and associates will be notified of the determination. Associates must not use a tool that Centric IT or Centric Legal has determined does not meet Centric Consulting's standards.

CONFIRMING ACCURACY:

Given the nature of generative AI tools (which include both CAAT and non-CAAT AI tools), the output may not always be accurate or reliable. Associates are responsible for verifying the accuracy and appropriateness of AI-generated content before using the results. This includes, but is not limited to, fact-checking information, reviewing for potential biases, and ensuring the content aligns with Centric Consulting's standards and values. Associates should not solely rely on AI-generated content for decision-making purposes without conducting an appropriate level of review and validation. If there are any doubts about the accuracy or appropriateness of AI-generated content, associates are encouraged to seek guidance from their supervisors or relevant subject matter experts.

This obligation applies with particular force in human resources contexts. AI-generated summaries, assessments, or comparative analyses of candidates or employees must never serve as the sole or primary basis for any employment decision. The associate responsible for the relevant hiring or management decision must independently review and validate all AI-generated outputs before acting on them, and must document that review as part of the standard decision-making record.

PROCUREMENT, PROVISIONING, AND REIMBURSEMENT:

All AI subscriptions, access to AI service APIs, and related AI services for Centric work must be provisioned through IT. Individual subscriptions should not be purchased directly. Existing independently expensed subscriptions should be canceled where feasible and reprovisioned through IT. Centric will not reimburse AI-related expenses unless the expense was approved in advance by IT.

COMPLIANCE AND ENFORCEMENT

Associates must promptly report any actual or suspected violation of this policy, including any inadvertent disclosure of confidential, proprietary, or personally identifiable information to an AI tool, to Centric IT at CentricIT@centricconsulting.com and to Centric Legal.

Centric Consulting will not retaliate against any associate who, in good faith, reports a suspected violation of this policy by another associate or raises a concern about AI tool use. Associates who fail to report known violations may be subject to disciplinary action in addition to any discipline arising from the underlying violation.

Violations of this policy may result in disciplinary action, including termination of employment. Centric Consulting reserves the right to monitor and audit the use of AI tools to ensure compliance with this policy.

For any inquiries, clarifications, or concerns regarding this policy, please reach out to our IT department at CentricIT@centricconsulting.com.

POLICY REVIEW AND UPDATES

Centric will review this policy periodically, and with increased frequency if material changes in applicable law, Company technology practices, or the AI tool landscape warrant an interim review. Centric Legal and Centric IT will jointly own the review process and will present any recommended updates to senior leadership for approval. Associates will be notified of any material changes to this policy within a reasonable time after those changes are approved.

SCHEDULE A – CENTRIC AI APPROVED TOOLS

The current list of Centric AI Approved Tools (“CAATs”) is maintained in Schedule A – Centric AI Approved Tools (CAAT) on the Lounge SharePoint site:

[https://centricconsultingllc.sharepoint.com/sites/TheLounge/SitePages/Centric-AI-Approved-Tools-\(CAAT\).aspx](https://centricconsultingllc.sharepoint.com/sites/TheLounge/SitePages/Centric-AI-Approved-Tools-(CAAT).aspx)

Associates must refer to the current Schedule A before using an AI tool client-specific, proprietary, or confidential information. Any AI tool not listed on Schedule A should be treated as a non-CAAT unless and until approved by Centric IT and Centric Legal.

ACKNOWLEDGEMENT

By using AI tools and services in the workplace, associates acknowledge that they have read, understood, and agree to comply with this policy.

Version Control

CREATED	
LAST REVIEWED/UPDATED	August 26, 2026
VERSION	2.0
AUTHOR	Joseph Ours
REVIEWED BY	Brian Sieberth
EFFECTIVE DATE	August 2026