
ARTIFICIAL INTELLIGENCE POLICY

Sage Oak Charter Schools ("SOCS" or the "Charter School") adopts this Artificial Intelligence (AI) Policy to guide the responsible use of AI technologies by employees and others who access SOCS systems or data in a non-instructional capacity. Contractors shall comply with this Policy and applicable data privacy laws as a condition of their engagement with SOCS.

SOCS recognizes that AI has the potential to enhance school operations, improve staff productivity, and support the efficient delivery of services. However, its use must be carefully managed to protect sensitive data, maintain public trust, and ensure that human judgment remains central to consequential decisions.

This policy applies to all employees, contractors, and vendors using AI tools or systems in the context of SOCS operations, administration, or technology environment. It does not govern instructional or student-facing AI use, which is addressed in a separate policy.

DEFINITION

Artificial Intelligence ("AI") refers to systems that use algorithms, data, and computational processes to perform complex tasks such as problem-solving, learning, reasoning, understanding natural language, and recognizing patterns. This includes generative AI models, machine learning applications, automated content tools, and related services or integrations across platforms, devices, and systems.

GUIDING PRINCIPLES

1. **Human-Centered Design:** AI use is intended to augment, not replace, human judgment and professional accountability. Employees remain responsible for verifying the factual accuracy, legality, appropriateness, and bias of any AI-generated output prior to use. No AI-generated work product may be used in an official capacity without human review.
2. **Privacy and Data Security:** Personally Identifiable Information (PII), protected health information, personnel records, financial data, and other sensitive or confidential information shall not be entered into unapproved AI tools. All tools must meet applicable federal and state data privacy requirements, including but not limited to the Family Educational Rights and Privacy Act (FERPA) and the Children's Online Privacy Protection Act (COPPA). Specific prohibited data inputs are defined in CTO Procedure 3160-P2.
3. **Equity and Access:** AI tools should support equitable outcomes. Tools that demonstrate or are known to produce biased outputs shall not be approved for use. All AI-generated content used in official communications or decisions shall be reviewed by staff for bias before use or disclosure. AI tools adopted by SOCS should support accessibility standards and shall not create barriers for individuals with disabilities.
4. **Transparency and Disclosure:** Employees shall not represent AI-generated content as solely their own original work. Where AI contributed substantially to a work product, employees remain fully accountable for its accuracy, legality, and appropriateness. Routine assistance from tools that provide spelling, grammar, or clarity suggestions does not require disclosure. Disclosure standards are defined in CTO Procedure 3160-P1.

ARTIFICIAL INTELLIGENCE POLICY

5. **Compliance:** All AI use must comply with applicable federal and state law, SOCS board policy, and contractual obligations. This includes but is not limited to FERPA, COPPA, the California Consumer Privacy Act (CCPA), and Ed Code requirements governing data privacy and security.
6. **Meeting Records:** AI-generated automated notetaking, including summaries, transcripts, drafts, or minutes, is considered a temporary working document and shall not be retained or treated as an official record of a meeting.

TOOL VETTING AND APPROVAL

Employees shall use only AI tools that have been vetted and approved through the SOCS technology governance process. Unapproved tools may not be used for any SOCS business, including administrative tasks, communications, data analysis, or workflow automation.

Employees shall not modify, disable, or circumvent privacy, security, or data protection settings on any AI tool used in connection with SOCS business.

Approved tools are maintained in the SOCS Approved AI Tool Registry, published and updated by the CTO. The registry identifies approved use cases and conditions for each tool. The CTO may add or remove tools from the registry at any time.

PERMISSIBLE AND PROHIBITED USE

Employees may use approved AI tools for non-instructional purposes including drafting and editing communications and administrative documents, summarizing or organizing non-confidential information, scheduling support, workflow automation, data analysis using appropriately protected data, research and professional development support, and translation and communication support for family and community engagement.

The following uses are prohibited under any circumstances:

- a. Entering protected student data, PII, personnel records, financial account data, or other confidential information into any unapproved AI tool;
- b. Using AI as the **sole basis** for consequential decisions involving employment, personnel actions, discipline, enrollment, accommodations, special education services, staffing, performance evaluation, complaints, investigations, or access to services. Human review and professional judgment are required before any such determination is made;
- c. Using unapproved AI tools for any SOCS-related work, regardless of whether the task is considered routine; and
- d. Using any AI system to access, create, or display harmful or inappropriate matter that is threatening, obscene, disruptive, or sexually explicit, or that could be construed as harassment or disparagement of others based on their race/ethnicity, national origin, sex, gender, sexual orientation, age, disability, religion, or political beliefs or interact with the AI in a manner that supports any of the above; and

ARTIFICIAL INTELLIGENCE POLICY

- e. Using AI tools in any manner that violates applicable law, board policy, or SOCS contractual obligations.

INCIDENT REPORTING

Employees must report suspected data exposures or AI system failures to the IT Department within 24 hours of discovery. The IT Department will notify the CTO, who will determine the appropriate response.

TRAINING AND SUPPORT

SOCS will provide ongoing professional development to employees on the responsible use of AI tools, including data privacy obligations, permitted and prohibited uses, and how to identify and report concerns. Training will be updated as tools, risks, and best practices evolve.

When an employee violates SOCS policy, regulation, or the SOCS Employee Acceptable Use Agreement, SOCS may suspend, revoke, or limit the employee's access to or use of AI tools, as appropriate. Inappropriate use may also result in disciplinary and/or legal action, consistent with applicable law and SOCS policy.