

## Sample Policy

### **USE OF ARTIFICIAL INTELLIGENCE (AI)**

**WHEREAS**, Local Education Agency (“LEA”) has created the following policies for all employees who may have access to and/or utilize Artificial Intelligence (“AI”). These policies also apply to volunteers, coaches, and others who interact in an electronic format with students and employees of the LEA and its member school districts (“District”);

**WHEREAS**, the employee acknowledges that AI is intended for only professional and responsible use by employees and students;

**NOW THEREFORE**,

### **TERMS AND CONDITIONS OF THIS POLICY**

Artificial Intelligence is a system of machine learning that is capable of performing complex and original tasks such as problem-solving, learning, reasoning, understanding natural language, and recognizing patterns in data. AI systems use algorithms, data, and computational power to simulate cognitive functions and make autonomous decisions, enabling them to perform a wide range of tasks and improve their performance over time through learning and adaptation.

The LEA recognizes that the use of AI can, when used appropriately, enhance student learning by improving the efficiency of education, providing new and creative ways to support learning, and encourage independent research, curiosity, critical thinking, and problem-solving.

The LEA authorizes staff members to utilize and permit students to utilize ethical and legal use of AI as a supplemental tool to support and expand on classroom instruction, facilitate personalized learning opportunities, and increase educational and learning opportunities, in accordance with the terms of this Policy.

### **Guidelines for Use**

The LEA has developed the following guidelines and protocols for the use of AI:

1. Before allowing students to use a specific AI platform in the classroom and before using an AI tool as a resource, employees should ensure that the AI system has been vetted and approved by the District or otherwise meets the District’s safety standards.
2. When applicable, the District should attain parental consent before offering certain open AI services to students.
3. Evaluation of an AI tool may include whether it:
  - a. is an open or closed environment for purposes of data collection;
  - b. has a privacy setting where data resharing can be limited or blocked;
  - c. meets current student data privacy standards;

- d. can be offered in an equitable manner;
  - e. any inherent bias can be minimized or eliminated; and
  - f. has safeguards in place to confirm that accurate and factually correct information can be provided.
4. Any use of AI in the classroom or on class assignments must align with the teachers' instructions and use expectations. Teachers will clarify whether students are prohibited from using AI in an assignment. Teachers will guide and monitor student use of AI, ensuring that it aligns with the District's guidelines and policies, including the District's Acceptable Use Policy.
  5. Use of an AI system must comply with the Family Educational Rights and Privacy Act. (FERPA) (20 USC 1232g; 34 CFR Part 99.)
  6. Any student use of AI on schoolwork must be cited to as any other source and may not be submitted as the student's original work.
  7. User should not solely rely on AI as a fact-checker to confirm their work or research as it may not always provide accurate or up-to-date information.

Users are prohibited from:

1. 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.
2. Sharing confidential information or personally identifiable information with the AI system of another student, staff member, or other person. AI information should not be shared with the intent to threaten, intimidate, harass, or ridicule that person. Personally identifiable information includes, but is not limited to, a person's name, address, email address, telephone number, Social Security number, or other personally identifiable information.

Whenever a user is found to have violated District Board Policy, Administrative Regulation, or the District's Acceptable Use Agreement, the principal or designee may cancel or limit a user's privileges with respect to their use of AI, as appropriate. Inappropriate use may also result in disciplinary action and/or legal action in accordance with law and Board policy.

### **Internet Safety**

The Superintendent or designee shall ensure that all District computers or devices with access to AI have protection measures to protect against access to materials that are obscene, contain child pornography, or are harmful to minors. (20 USC 6777; 47 USC 254; 47 CFR 54.520.)

Harmful matter includes matter, taken as a whole, which to the average person, applying contemporary statewide standards, appeals to the prurient interests and is matter which depicts or describes, in a patently offensive way, sexual conduct and which lacks serious literary, artistic, political, or scientific value for minors. (Penal Code 313.)

The Superintendent or designee, with input from students and appropriate staff, shall regularly review and update procedures to enhance the safety and security of students using AI and to help ensure that the District adapts to changing technologies and circumstances.

**Policy Reference Disclaimer:**

These references are not intended to be part of the policy itself, nor do they indicate the basis or authority for the board to enact this policy. Instead, they are provided as additional resources for those interested in the subject matter of the policy.

<b>State</b>	<b>Description</b>
Ed. Code 49073.6	Student records; social media
Ed. Code 51006	Computer education and resources
Ed. Code 51007	Programs to strengthen technological skills
Ed. Code 60044	Prohibited instructional materials
Pen. Code 313	Harmful matter
Pen. Code 502	Computer crimes; remedies
Pen. Code 632	Eavesdropping on or recording confidential communications
Pen. Code 653.2	Electronic communication devices; threats to safety
<b>Federal</b>	<b>Description</b>
15 USC 6501-6506	Children’s Online Privacy Protection Act
16 CFR 312.1-312.12	Children’s Online Privacy Protection Act
20 USC 1232g	Family Educational Rights and Privacy Act
34 CFR Part 99	Family Educational Rights and Privacy Act
20 USC 7101-7122	Student Support and Academic Enrichment Grants
20 USC 7131	Internet Safety
47 CFR 54.520	Internet safety policy and technology protection measures; E-rate discounts
47 USC 254	Universal service discounts (E-rate)