ACCEPTABLE USE AGREEMENT AND RELEASE OF COUNTY OFFICE OF EDUCATION FROM LIABILITY (EMPLOYEES)

The Nevada County Office of Education (COE) authorizes COE employees to use technology, as defined in County Superintendent Policy 4040 - Acceptable Use of Technology. The use of COE technology is a privilege permitted at the COE's discretion and is subject to the conditions and restrictions set forth in applicable local policies, administrative regulations, and this Acceptable Use Agreement. The COE reserves the right to suspend access at any time, without notice, for any reason. However, the COE shall not prevent or restrict access to an employee's mobile or other communications device(s) if there is a need to seek emergency assistance, assess the safety of a situation, or communicate with a person to confirm the person's safety.

The COE expects all employees to use technology responsibly in order to avoid potential problems and liability. The COE may place reasonable restrictions on the sites, material, and/or information that employees may access through the system.

The COE makes no guarantee that the functions or services provided by or through the COE will be without defect. In addition, the COE is not responsible for financial obligations arising from unauthorized use, or misuse, of the system.

Each employee who is authorized to use COE technology shall sign this Agreement, which indicates that the employee has read and understands this Agreement and County Superintendent Policy 4040 - Acceptable Use of Technology.

Employee Obligations and Responsibilities

Employees are expected to use COE technology safely, responsibly, and primarily for work-related purposes and in accordance with the accompanying County Superintendent Policy and applicable copyright laws. Any incidental personal use of COE technology shall not interfere with COE business and operations, the work and productivity of any COE employee, or the safety and security of COE technology.

The COE is not responsible for any loss or damage incurred by an employee as a result of the employee's personal use of COE technology. The employee in whose name COE technology is issued is responsible for its proper use at all times. Employees shall not share their assigned online services account information, passwords, or other information used for identification and authorization purposes, and shall use the system only under the account to which they have been assigned. Employees shall not gain unauthorized access to the files or equipment of others, access electronic resources by using another person's name or electronic identification or send anonymous electronic communications. Furthermore, employees shall not attempt to access any

data, documents, emails, or programs in the COE's system for which they do not have authorization.
Employees are prohibited from using COE technology for improper purposes, including, but not limited to, use of COE technology to:

1. Access, post, display, create, or otherwise use material that is discriminatory, defamatory, obscene, sexually explicit, harassing, intimidating, threatening, or disruptive
2. Disclose or in any way cause to be disclosed confidential or sensitive COE, employee, or student information without prior authorization from a supervisor
3. Engage in personal commercial or other for-profit activities without permission
4. Engage in unlawful use of COE technology for political lobbying
5. Infringe on copyright, license, trademark, patent, or other intellectual property rights
6. Intentionally disrupt or harm COE technology or other COE operations (such as destroying COE equipment, placing a virus on COE computers, adding or removing a computer program without permission, changing settings on shared computers)
7. Install unauthorized software
8. Engage in or promote unethical practices or violate any law or local policy, administrative regulation, or local practice

Email Use

All work-related communications must be conducted using the COE-provided email address. Employees are not permitted to use non-COE email accounts for any work-related communications. All email sent or received by an individual with account(s) with NCSOS is the property of NCSOS and may be requested by the immediate supervisor, the superintendent or their designee, and examined with or without reason or warning.

Multi-Factor Authentication

Employees must not share their passwords or account information with others. Employees are required to utilize Multi Factor Authentication (MFA) on their COE issued accounts and maintain a secure password that meets the IT department’s password requirements. Employees must report any security breaches or suspicious activity to the IT department immediately. Reference the NCSOS MFA Policy

Privacy

Since the use of COE technology is intended for use in conducting COE business, no employee should have any expectation of privacy in any use of COE technology.

The COE reserves the right to monitor and record all use of COE technology, including, but not limited to, access to the Internet or social media, Internet searches, browsing history, use of artificial intelligence, communications sent or received from COE technology, or other uses

within the jurisdiction of the COE. Such monitoring/recording may occur at any time without prior notice for any legal purposes including, but not limited to, record retention and distribution and/or investigation of improper, illegal, or prohibited activity. Employees should be aware that, in most instances, their use of COE technology (such as web searches or emails) cannot be erased or deleted.
All passwords created for or used on any COE technology are the sole property of the COE. The creation or use of a password by an employee on COE technology does not create a reasonable expectation of privacy.

Personally Owned Devices

The COE works to ensure that all hardware and software meets specifications that comply with cybersecurity standards as well as the standards of the IT department. The use of personally owned software or hardware may be used only after proper assessment and approval by the IT department.

If an employee uses a personally owned device to access COE technology or conduct COE business, the employee shall abide by all applicable local policies, administrative regulations, and this Agreement. Any such use of a personally owned device may subject the contents of the device, and any communications sent or received on the device to disclosure pursuant to a lawful subpoena or public records request. Records Any electronically stored information generated or received by an employee which constitutes a COE or student record shall be classified, retained, and destroyed in accordance with applicable policies and regulations addressing the retention of COE or student records.

Record Privacy and Sensitive Information

It is each employee's responsibility to safeguard sensitive information from unauthorized persons as required by local, state, and Federal Law. Employees must refrain from sending or receiving Personally Identifiable Information (PII) via email. PII includes, but is not limited to:

- Addresses
- Social security numbers
- Credit Card Information
- Any other information that can be used to identify an individual.

If it is necessary to share PII, Employees must use secure methods approved by the COE.

Reporting

If an employee becomes aware of any security problem (including, but not limited to, a cyberattack, phishing, or any compromise of the confidentiality of any login or account information), or misuse of COE technology, the employee shall immediately report such information.

Consequences for Violation

Violations of the law, local policy, or this Agreement may result in revocation of an employee's access to COE technology and/or discipline, up to and including termination. In addition, violations of the law, local policy, or this agreement may be reported to law enforcement agencies as appropriate.

Employee Acknowledgment

I have received, read, understand, and agree to abide by this Agreement, County Superintendent Policy 4040 - Acceptable Use of Technology, and other applicable laws and COE policies and regulations governing the use of COE technology. I understand that there is no expectation of privacy when using COE technology or when my personal electronic devices use COE technology. I further understand that any violation may result in revocation of user privileges, disciplinary action, and/or appropriate legal action.

I hereby release the COE, its personnel, the County Superintendent of Schools, and the County Board of Education from any and all claims and damages arising from my use of COE technology or from the failure of any technology protection measures employed by the COE.

Name: _____ Position: _____
(Please print)

School/Work Site: _____

Signature: _____ Date: _____