NVUSD EMPLOYEE ACCEPTABLE USE AGREEMENT
AND RELEASE OF DISTRICT FROM LIABILITY

The Napa Valley Unified School District authorizes district employees to use technology owned or otherwise provided by the district as necessary to fulfill the requirements of their position. The use of district technology is a privilege permitted at the district's discretion and is subject to the conditions and restrictions set forth in applicable Board policies, administrative regulations, and this Acceptable Use Agreement. The district reserves the right to suspend access at any time, without notice, for any reason.

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

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

Each employee who is authorized to use district technology shall sign this Acceptable Use Agreement as an indication that he/she has read and understands the agreement.

Definitions:
District technology includes, but is not limited to, computers, the district's computer network including servers and wireless computer networking technology (Wi-Fi), the Internet, email, USB drives, wireless access points (routers), tablets, computers, smartphones, and smart devices, telephones, cellular telephones, personal digital assistants, MP3 players, wearable technology, any wireless communication device including emergency radios, and/or future technological innovations, whether accessed on or off-site or through district-owned or personally owned equipment or devices.

Responsible Use and Payment for Damage:
The Employee acknowledges that they are responsible for any damage caused to the device due to their intentional acts, negligence, misuse, abuse, or violation of the School District's policies. In the event of accidental damage caused by the Employee, the Employee may be responsible for the cost of repair or replacement of the device. The Employee agrees to promptly report any damage caused to the device to the designated School District authority.

Employee Obligations and Responsibilities:
Employees are expected to use district technology safely, responsibly, and primarily for work-related purposes. Any incidental personal use of district technology shall not interfere with district business and operations, the work and productivity of any district employee, or the safety and security of district technology. The district is not responsible for any loss or damage incurred by an employee as a result of his/her personal use of district technology.

The employee in whose name district 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 district's system for which they do not have authorization.
Employees are prohibited from using district technology for improper purposes, including, but not limited to, the use of district technology to:

1. Access, post, display, 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 district, employee, or student information without prior authorization from a supervisor
3. Engage in personal commercial or other for-profit activities without permission of the Superintendent or designee
4. Engage in unlawful use of district technology for political lobbying
5. Infringe on copyright, license, trademark, patent, or other intellectual property rights
6. Intentionally disrupt or harm district technology or other district operations (such as destroying district equipment, placing malware on district computers or networking devices, adding or removing a computer program without permission, changing settings on shared computers)
7. Install unauthorized software or hardware
8. Engage in or promote unethical practices or violate any law or Board policy, administrative regulation, or district practice

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

The district reserves the right to monitor and record all use of district technology, including, but not limited to, access to the Internet or social media, communications sent or received from district technology, or other uses within the jurisdiction of the district. 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 district technology (such as web searches or emails) cannot be erased or deleted.

All passwords created for or used on any district technology are the sole property of the district. The creation or use of a password by an employee on district technology does not create a reasonable expectation of privacy.

Personally Owned Devices:
If an employee uses a personally owned device to access district technology or conduct district business, he/she shall abide by all applicable Board policies, administrative regulations, and this Acceptable Use 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. The district or district staff is not responsible for service, repair, or troubleshooting of personally owned devices.

Records:
Any electronically stored information generated or received by an employee that constitutes a district or student record shall be classified, retained, and destroyed in accordance with BP/ AR 3580 - District Records, BP I AR 5125 - Student Records, or other applicable policies and regulations addressing the retention of district or student records.

Use of Artificial Intelligence Tools:
Employees are strictly prohibited from inputting, uploading, or sharing any District confidential information or any Personally Identifiable Information (“PII”) of students, employees, or any other individual into AI tools. PII includes but is not limited to, names, addresses, phone numbers, and any other information that could potentially identify an individual. PII specifically includes the definition in the Family Educational Rights and Privacy Act (“FERPA” 34 C.F.R. §99.3). “Confidential Information” includes, but is not limited to, trade secrets, proprietary data, financial information, strategic plans, and any other sensitive information pertinent to the District's operations.

An AI tool refers to any software, application, or platform that utilizes machine learning, natural language processing, or any form of artificial intelligence to process data or generate content. Examples of such AI tools include, but are not limited to, chatbots, virtual assistants, and content generation tools such as ChatGPT, Google Bard, Microsoft Azure, or Copilot. Employees should be aware that both deliberate inputting, uploading, or sharing of PII with any AI tool is prohibited, and inadvertent inputting, uploading, or sharing of PII through, for example, an automatic AI-notetaking feature on a video platform. Employees are advised to turn off any and all automatic AI features on any software, applications, platforms, or tools that they use.

Failure to comply with this policy will result in disciplinary action, up to and including termination of employment.

Reporting:
If an employee becomes aware of any security problem (such as any compromise of the confidentiality of any login or account information) or misuse of district technology, he/she shall immediately report such information to the Superintendent or designee. The employee shall

report any international travel no later than 7 days before the date of travel in order to allow for access to district email outside of the United States and Mexico.

Consequences for Violation:
Violations of the law, Board policy, or this Acceptable Use Agreement may result in revocation of an employee's access to district technology and/or discipline, up to and including termination. In addition, violations of the law, Board 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 Acceptable Use Agreement, BP/AR 4040 - Employee Use of Technology, and other applicable laws and district policies and regulations governing the use of district technology. I understand that there is no expectation of privacy when using district technology or when my personal electronic devices use district 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 district and its personnel from any and all claims and damages arising from my use of district technology or from the failure of any technology protection measures employed by the district.

NVUSD
NAPA VALLEY UNIFIED SCHOOL DISTRICT

ACUERDO DE USO ACEPTABLE DE EMPLEADO DEL NVUSD
Y EXENCIÓN DE RESPONSABILIDAD DEL DISTRITO

El Distrito Escolar Unificado del Valle de Napa autoriza a los empleados del distrito a utilizar tecnología de su propiedad o proporcionada por el distrito según sea necesario para cumplir los requisitos de su puesto. El uso de tecnología del distrito es un privilegio permitido a discreción del distrito y está sujeto a las condiciones y restricciones establecidas en las normativas del Consejo, en las regulaciones administrativas aplicables y en este Acuerdo de Uso Aceptable. El distrito se reserva el derecho a suspender el acceso en cualquier momento, sin aviso, por cualquier motivo.

El distrito espera que todos los empleados usen la tecnología responsablemente para evitar problemas y responsabilidades potenciales. El distrito puede poner restricciones razonables en las páginas, materiales o información a la que los empleados pueden acceder a través del sistema.

El distrito no garantiza que las funciones o servicios prestados por el distrito o a través de él carezcan de defectos. Además, el distrito no es responsable de las obligaciones financieras derivadas del uso no autorizado del sistema.

Cada empleado que esté autorizado para usar la tecnología del distrito deberá firmar este Acuerdo de Uso Aceptable como indicación de que ha leído y comprende el acuerdo.

Definiciones:
La tecnología del distrito incluye, pero no está limitada a: computadoras, red informática del distrito inclusive servidores y tecnología de red informática inalámbrica (wifi), internet, correo electrónico, memorias USB, puntos de acceso inalámbricos (rúters), tabletas, computadoras, teléfonos inteligentes y dispositivos inteligentes, teléfonos, teléfonos celulares, asistentes personales digitales, reproductores MP3, tecnológica portátil, cualquier dispositivo de comunicación inalámbrica inclusive radios de emergencia y/o futuras innovaciones tecnológicas, independientemente de si se accede en o fuera de las instalaciones o mediante equipamiento o dispositivos de propiedad del distrito o de propiedad personal.

Uso responsable y pago por daños:
El empleado reconoce que es responsable de cualquier daño causado al dispositivo debido a sus actos intencionados, negligencia, mal uso, abuso o infracción de las normativas del Distrito

Escolar. En caso de daño accidental causado por el empleado, este podrá ser responsable del coste de reparación o sustitución del aparato. El empleado se compromete a informar inmediatamente de cualquier daño causado al dispositivo a la autoridad designada por el Distrito Escolar.

Obligaciones y responsabilidades del empleado:
Se espera que los empleados usen la tecnología del distrito de manera segura, responsable y principalmente con propósitos relacionados con el trabajo. Cualquier uso personal incidental de la tecnología del distrito no deberá interferir con los negocios y operaciones del distrito, el trabajo y la productividad de cualquier empleado del distrito, o la seguridad y protección de la tecnología del distrito. El distrito no es responsable de ninguna pérdida o daño sufrido por un empleado como resultado de su uso personal de la tecnología del distrito.

El empleado bajo cuyo nombre se presta la tecnología del distrito es responsable de su uso apropiado en todo momento. Los empleados no compartirán su información sobre cuentas de servicios online asignadas, contraseñas u otra información usada con propósitos de identificación y autorización, y usará el sistema solo con la cuenta que se le ha asignado. Los empleados no obtendrán acceso no autorizado a los archivos o equipos de otros, no accederán a los recursos electrónicos utilizando el nombre o la identificación electrónica de otra persona, ni enviarán comunicaciones electrónicas anónimas. Además, los empleados no intentarán acceder a ningún dato, documento, correo electrónico o programa del sistema del distrito para el que no tengan autorización.
Se prohíbe que los empleados usen tecnología del distrito con propósitos impropios, inclusive, pero sin estar limitado a, el uso de la tecnología del distrito para:

1. Acceder, publicar, mostrar o usar de cualquier otro modo material discriminatorio, difamatorio, obsceno, sexualmente explícito, intimidante, amenazador o disruptivo
2. Divulgar o hacer que se divulgue de cualquier modo información confidencial o delicada del distrito, de los empleados o de los estudiantes sin la autorización previa de un supervisor
3. Participar en actividades comerciales personales u otras actividades lucrativas sin el permiso de la Superintendente o de la persona designada
4. Participar en el uso ilegal de la tecnología del distrito para grupos de presión política
5. Infringir derechos de autor, licencia, marca registrada, patente u otros derechos de la propiedad intelectual.
6. Alterar o dañar intencionalmente la tecnología del distrito u otras operaciones del distrito (como destruir equipamiento del distrito, colocar malware en las computadoras o dispositivos de red del distrito, añadir o eliminar un programa informático sin permiso, cambiar la configuración de computadoras compartidas)
7. Instalar software o hardware no autorizado
8. Participar en o fomentar prácticas no éticas o que infrinjan cualquier ley o normativa del Consejo, regulación administrativa o práctica del distrito

Privacidad:

Dado que el uso de la tecnología del distrito tiene la intención de emplearse para realizar las funciones del distrito, ningún empleado tendrá expectativa alguna de privacidad mientras haga cualquier uso de la tecnología del distrito.

El distrito se reserva el derecho a vigilar y registrar todos los usos de la tecnología del distrito, inclusive, pero sin estar limitado a: acceso a internet o redes sociales, comunicaciones enviadas desde o recibidas en tecnología del distrito, u otros usos dentro de la jurisdicción del distrito. Dicha vigilancia/grabación puede tener lugar en cualquier momento sin notificación previa por cualquier motivo legal, inclusive, pero sin estar limitado a, retención y distribución de registros y/o investigación de actividad impropia, ilegal o prohibida. Los empleados deberían saber que, en la mayoría de los casos, su uso de tecnología del distrito (como búsquedas en la red o correos electrónicos) no puede ser borrado ni eliminado.

Todas las contraseñas creadas para o usadas en cualquier tecnología del distrito son propiedad exclusiva del distrito. La creación o uso de una contraseña por parte de un empleado en tecnología del distrito no crea una expectativa razonable de privacidad.

Dispositivos de propiedad personal:
Si un empleado usa un dispositivo de propiedad personal para acceder a tecnología del distrito o llevar a cabo funciones del distrito, deberá cumplir todas las normativas del Consejo, regulaciones administrativas y con este Acuerdo de Uso Aceptable. Cualquier utilización de un dispositivo de propiedad personal puede exponer los contenidos del dispositivo y cualquier comunicación enviada o recibida en el dispositivo a su publicación, de acuerdo con un requerimiento legal o solicitud de registros públicos. El distrito o el personal del distrito no son responsables del servicio, reparación o solución de problemas de los dispositivos de propiedad personal.

Registros:
Cualquier información almacenada electrónicamente generada o recibida por un empleado que constituya un registro del distrito o de un alumno se clasificará, conservará y destruirá de acuerdo con BP/AR 3580 - Registros del Distrito, BP/AR 5125 - Registros de Alumnos, u otras normativas y reglamentos aplicables que aborden la conservación de los registros del distrito o de los alumnos.

Uso de herramientas de inteligencia artificial:
Los empleados tienen estrictamente prohibido introducir, cargar o compartir cualquier información confidencial del Distrito o cualquier Información de Identificación Personal (“IIP”) de estudiantes, empleados o cualquier otro individuo en herramientas de IA. La IIP incluye, entre otros, nombres, direcciones, números de teléfono y cualquier otra información que pueda identificar potencialmente a una persona. La IIP incluye específicamente la definición de la Ley de Privacidad y Derechos Educativos de la Familia (“FERPA” 34 C.F.R. §99.3). “Información Confidencial” incluye, pero no se limita a, secretos comerciales, datos privados, información financiera, planes estratégicos y cualquier otra información sensible pertinente a las operaciones del Distrito.

Una herramienta de IA se refiere a cualquier software, aplicación o plataforma que utilice el aprendizaje automático, el procesamiento del lenguaje natural o cualquier forma de inteligencia artificial para procesar datos o generar contenidos. Algunos ejemplos de estas herramientas de IA son, entre otros, los chatbots, los asistentes virtuales y las herramientas de generación de contenidos como ChatGPT, Google Bard, Microsoft Azure o Copilot. Los empleados deben ser conscientes de que está prohibido tanto introducir, cargar o compartir información de identificación personal de manera deliberada con cualquier herramienta de IA, como introducir, cargar o compartir información de identificación personal de manera inadvertida a través de, por ejemplo, una función automática de toma de notas de IA en una plataforma de vídeo. Se aconseja a los empleados que desactiven todas y cada una de las funciones automáticas de IA en cualquier software, aplicación, plataforma o herramienta que utilicen.

El incumplimiento de esta política dará lugar a medidas disciplinarias, que pueden incluir el despido.

Informe:
Si un empleado tiene constancia sobre cualquier problema de seguridad (como cualquier riesgo de la confidencialidad de cualquier ingreso o información sobre cuentas) o uso indebido de la tecnología del distrito, deberá informar inmediatamente sobre esto a la Superintendente o persona designada. El empleado deberá informar de cualquier viaje internacional a más tardar 7 días antes de la fecha del viaje para permitir el acceso al correo electrónico del distrito fuera de Estados Unidos y México.

Consecuencias por infracción:
Las infracciones de la ley, normativas del Consejo, o de este Acuerdo de Uso Aceptable pueden conllevar la revocación del acceso de un empleado a la tecnología del distrito y/o disciplina, hasta e inclusive rescisión del contrato. Además, las infracciones de la ley, de las normativas del Consejo, o de este acuerdo, pueden comunicarse a las agencias y cuerpos de seguridad según proceda.

Reconocimiento del empleado:
He recibido, leído, comprendido y estoy de acuerdo en cumplir este Acuerdo de Uso Aceptable, BP/AR 4040 - Uso de Tecnología del Empleado y cualesquiera otras leyes, normativas y regulaciones del distrito que gobiernen el uso de tecnología del distrito. Comprendo que no hay ninguna expectativa de privacidad cuando se utiliza la tecnología del distrito o cuando mis dispositivos electrónicos personales utilizan la tecnología del distrito. Además, también comprendo que cualquier infracción puede conllevar la revocación de privilegios de usuario, acción disciplinaria, y/o acción legal apropiada.

Por la presente, eximo al distrito y a su personal de cualquier reclamación y daños derivados de mi uso de la tecnología del distrito o del fallo de cualquier medida de protección tecnológica empleada por el distrito.