

DISTRITO ESCOLAR DEL CONDADO DE CLARK

Política de Uso Aceptable

**DISTRITO ESCOLAR
DEL CONDADO DE CLARK**



**DISTRITO ESCOLAR
DEL CONDADO DE CLARK**

Visión

*Todos los estudiantes progresan en la escuela y se gradúan preparados
para tener éxito y contribuir en una sociedad global diversa.*

POLÍTICA DE USO ACEPTABLE

Los recursos de la red informática, proporcionados por el Distrito Escolar del Condado de Clark (Distrito), posibilitan la comunicación con comunidades electrónicas alrededor del mundo. Estos recursos de la red informática incluyen internet, correo electrónico, sistemas basados en la nube y todos los demás proveedores de servicios a través del internet cuando se utilizan en un entorno educativo.

El uso de estos recursos electrónicos deberá ajustarse al propósito, la misión y las metas del Distrito, y se deben utilizar para propósitos profesionales o educativos. El propósito de proporcionar estos servicios es para facilitar el acceso a información y recursos, fomentar la excelencia educativa y mejorar la comunicación.

El Internet es una red que conecta miles de computadoras de todo el mundo. El Internet puede traer un cúmulo de riquezas de material educativo al salón, pero también puede contener material que es cuestionable. El Distrito filtra los sitios web y los contenidos que se consideran inapropiados para los estudiantes de conformidad con las mejores prácticas de ciberseguridad y de la Ley de Protección de Menores en Internet (CIPA*). Sin embargo, ningún sistema de filtrado es perfecto. El Distrito no puede garantizar que el material inapropiado o cuestionable pueda ser completamente filtrado. Los padres y tutores deben considerar esto al decidir si permiten que sus hijos tengan acceso a los recursos de la red informática del Distrito.

Se proporciona esta Política de Uso Aceptable (AUP*) para que el personal, estudiantes y miembros de la comunidad que utilicen los recursos de la red informática sean conscientes de sus responsabilidades. El uso de estos recursos de red del Distrito es un privilegio, no un derecho.

TÉRMINOS Y CONDICIONES

A. Acceso a los Recursos de la Red del Distrito

1. El personal, los estudiantes y los miembros de la comunidad pueden tener acceso a los recursos de la red informática del Distrito. Este acceso, incluyendo la cuenta y la contraseña, no debe compartirse, asignarse ni transferirse a otra persona.
2. Los recursos de la red informática del Distrito están destinados únicamente a fines educativos oficiales del Distrito. El uso personal de estos recursos de la red informática está estrictamente prohibido (aparte del uso personal incidental como se establece en la Sección J de esta AUP). El uso indebido, incluido el uso no autorizado de los recursos de la red informática y los datos almacenados en ella para actividades personales, puede dar lugar a medidas disciplinarias, que pueden incluir la suspensión o terminación del acceso.
3. El Distrito requerirá periódicamente nueva información de registro y cuenta de la escuela, el personal y los miembros de la comunidad. Los usuarios adultos deben notificar a los administradores del sistema de cualquier cambio en la información de la cuenta (dirección, teléfono, nombre, etc.) dentro de quince (15) días hábiles.
4. Los empleados que infrinjan esta AUP están sujetos a medidas disciplinarias progresivas que pueden incluir el despido. Las infracciones de los estudiantes a esta AUP seguirán el proceso disciplinario del *Distrito Escolar del Condado de Clark de Preescolar al 12. ° Grado Código de Conducta Estudiantil*.
5. Al momento de la inscripción, cada estudiante recibirá acceso a los recursos de la red del Distrito a menos que un padre/ tutor indique explícitamente que el estudiante no debe tener acceso durante el proceso de inscripción en línea. Los padres o tutores pueden optar por renunciar al acceso a la red en cualquier momento previa solicitud por escrito.

6. Las cuentas proporcionadas por el Distrito (@nv.ccsd.net) se proporcionan para cumplir con las responsabilidades laborales y educativas dentro de la organización. Las cuentas deben usarse únicamente con fines laborales y/o educativos y no deben usarse para fines personales. Las cuentas proporcionadas por el Distrito no se pueden usar para registrarse en servicios personales como Facebook, TikTok, Instagram, etc.
7. El uso de servicios de transmisión (por ejemplo, entretenimiento, música, juegos) utilizando cuentas personales (que no sean del Distrito) está prohibido en la red del Distrito. Tener una cuenta personal con estos servicios no le permite utilizar el servicio para nada que no sea uso personal. El uso de estos servicios para o en el trabajo puede constituir una infracción de los derechos de autor. Por lo tanto, el acceso a estos servicios se restringirá para evitar cualquier infracción de la ley de derechos de autor y para mantener un uso adecuado de la red.
8. El acceso a los servicios de juegos en línea generalmente está restringido en la red del Distrito, con excepciones para programas educativos específicos y clubes patrocinados por escuelas que tienen aprobación previa. No se puede acceder a sitios o aplicaciones de juegos que no estén expresamente autorizados en la red. Las excepciones se administran caso por caso para respaldar fines educativos y minimizar el tráfico no educativo de red.
9. Los usuarios deben utilizar la autenticación multifactor (MFA*) al acceder a sistemas y recursos confidenciales, siempre que sea técnicamente posible, de conformidad con las políticas de seguridad del Distrito.
10. Los usuarios deben bloquear los dispositivos cuando están desatendidos y cerrar la sesión de los recursos de red después de cada sesión. Las contraseñas deben ser seguras,

únicas y cambiarse regularmente de acuerdo con las políticas de seguridad del Distrito.

11. Los usuarios deben usar contraseñas que cumplan con los requisitos de seguridad del Distrito y actualizarlas según sea necesario.
12. El Distrito proporciona una red de invitados para el uso temporal de visitantes. El acceso se limita a la navegación básica y está sujeto a la supervisión del Distrito. Los usuarios invitados no deben acceder a los sistemas internos del Distrito, transmitir datos confidenciales ni participar en actividades restringidas. El uso de los recursos de red por parte de los usuarios invitados es un privilegio, no un derecho.

B. Seguridad del Sistema

1. Los usuarios de computadoras no pueden ejecutar aplicaciones o archivos que creen un riesgo de seguridad para los recursos de la red informática del Distrito. Si los usuarios identifican un problema de seguridad, deben notificarlo inmediatamente a los administradores correspondientes.
2. Cualquier usuario que se considere razonablemente un riesgo de seguridad o que se descubra que tiene un historial comprobado de problemas con otras redes informáticas se le puede negar el acceso a los recursos de la red informática del Distrito.
3. Los usuarios deben informar de inmediato cualquier sospecha de acceso no autorizado a sus cuentas.
4. Está prohibido proporcionar acceso a la cuenta o compartir las credenciales de su cuenta con otra persona, ya sea deliberadamente o por negligencia.
5. Todos los usuarios deben informar de cualquier incidente de seguridad o sospecha de incidente (como infecciones de programa maligno, filtración de datos o acceso no

autorizado) inmediatamente al servicio de ayuda técnica. Los informes deben incluir todos los detalles relevantes y se revisarán de acuerdo con el protocolo de respuesta a incidentes del Distrito.

C. Respetando los Límites de los Recursos

1. El personal, los estudiantes y los miembros de la comunidad no publicarán cartas en cadena ni participarán en el envío de correo no deseado. El correo no deseado consiste en enviar mensajes a un gran número de personas o enviar un gran número de mensajes a una sola persona con la intención de irritar a los usuarios o interrumpir el sistema.
2. Los administradores del sistema se reservan el derecho de establecer un límite de almacenamiento en disco para los usuarios de la red.
3. A menos que se apruebe previamente, los usuarios son responsables de cualquier cargo telefónico, incluyendo, pero no limitado a, cargos de larga distancia, recargos por minuto (unidad) y/o costos de equipo o de línea incurridos por los usuarios al acceder a los recursos de la red informática.

D. Actividades Ilegales

1. El Distrito cooperará plenamente con los funcionarios locales, estatales o federales en cualquier investigación relacionada con actividades ilegales, que puede incluir información contenida en los recursos de red del Distrito.
2. Está prohibido vender o comprar bienes y servicios en los recursos de red del Distrito sin la aprobación previa del administrador correspondiente.
3. Está prohibido intentar obtener acceso no autorizado a los recursos de red del Distrito o ir más allá del acceso autorizado. Esto incluye intentar iniciar sesión a través de

la cuenta de otra persona o acceder a los archivos de otra persona.

4. El vandalismo resultará en la cancelación de privilegios a los recursos de la red informática del Distrito. El vandalismo se define como cualquier intento malicioso de dañar o destruir datos o equipos en cualquier red informática.
5. Está prohibido usar los recursos de la red informática del Distrito con la intención de negar a otros el acceso al sistema.
6. Se permitirá la publicidad en los recursos de la red informática del Distrito con la aprobación previa del administrador correspondiente.
7. La descarga, el uso, el alojamiento o la distribución de material y software con derechos de autor es ilegal y está prohibida en los recursos de la red informática del Distrito, a menos que se encuentre dentro de una excepción al uso de materiales con derechos de autor.

E. Propiedad Intelectual (Derechos de Autor)

1. Ningún material con derechos de autor debe colocarse en los recursos de la red informática del Distrito sin el permiso por escrito del propietario de los derechos de autor, a menos que se encuentre dentro de una excepción al uso de materiales con derechos de autor.
2. Ningún material protegido por derechos de autor (incluyendo música, juegos, videos y software) puede ser alojado o distribuido dentro o desde los recursos de la red informática del Distrito sin el permiso por escrito del propietario de los derechos de autor y debe ser aprobado por la División de Servicios de Tecnología y Sistemas de Información a menos que se encuentre dentro de una excepción al uso de materiales con derechos de autor.

3. Todos los usuarios de los recursos de la red del Distrito deben comprometerse a no enviar, publicar o mostrar ningún tipo de material que infrinja esta AUP.

F. Software

1. Solo los archivos de dominio público y los archivos para los que el autor ha dado su consentimiento por escrito para su distribución en línea pueden cargarse en las bibliotecas de software del Distrito.
2. Se prohíbe el software que tenga el propósito de dañar los recursos de red del Distrito u otros sistemas.
3. Es posible que se requiera que los usuarios usen un navegador de Internet aprobado por el Distrito u otro software para acceder a los recursos de la red informática.
4. Está prohibido el uso de software o recursos no aprobados para compartir archivos, incluidos sitios web de almacenamiento en la nube, sitios de torrents y otras opciones de redes entre pares.

G. Lenguaje

1. Se espera un lenguaje cortés y apropiado en todo momento.
2. Están prohibidos los mensajes abusivos.
3. El acoso está prohibido. El acoso es una conducta que es lo suficientemente grave, persistente o dominante como para afectar negativamente o tener el propósito o la consecuencia lógica de interferir con el programa educativo de un usuario o crear un entorno intimidatorio, hostil u ofensivo. El comportamiento que continúa después de que una persona es informada de su ofensa puede constituir evidencia de una intención de acoso. Si una persona le dice que deje de enviar mensajes, el remitente debe dejar de hacerlo.

H. Responsabilidad

1. El Distrito no garantiza las funciones o servicios realizados por los recursos de la red informática del Distrito. Los recursos se proporcionan “tal cual, según disponibilidad”.
2. Las opiniones, consejos, servicios y cualquier otra información proporcionada por terceros son solo para fines informativos. No se garantiza que sea correcto. Se insta a los usuarios a buscar asesoramiento profesional para situaciones individuales específicas.
3. Cualquier software disponible de los recursos de red del Distrito no está garantizado en cuanto a idoneidad, legalidad o rendimiento por parte del Distrito.
4. El personal, los estudiantes y los miembros de la comunidad acuerdan indemnizar y eximir de responsabilidad al Distrito por cualquier responsabilidad que surja de cualquier infracción de esta AUP.

I. Correo Electrónico y Conferencias en Tiempo Real

1. No es la intención de los administradores del sistema inspeccionar o divulgar el contenido del correo electrónico o los archivos de computadora enviados por un usuario a otro sin el consentimiento de ninguna de las partes, a menos que así lo requieran el Distrito, los funcionarios locales, estatales o federales. El correo electrónico no es privado. Al igual que con la comunicación escrita, los usuarios deben reconocer que no hay expectativas de privacidad para el correo electrónico.
2. Los usuarios no deben usar lemas, citas, bromas, imágenes, enlaces u otros elementos que no sean pertinentes a la información de contacto esencial relacionada con el empleo del distrito escolar al final del mensaje de correo electrónico o en el bloque de firma de correo electrónico.

3. Todos los usuarios deben informar de inmediato los mensajes inapropiados recibidos a: un maestro, supervisor o a los administradores del sistema.
4. Los estudiantes no deben revelar información personal como direcciones, números de teléfono, contraseñas o información financiera a otras personas. Si se identifica el trabajo del estudiante, solo se debe indicar el nombre, el grado y la escuela. No se puede publicar información privada sobre otra persona.
5. El Distrito no permite la grabación o transcripción de reuniones virtuales organizadas por el Distrito debido a preocupaciones incluyendo, pero no limitado a: la Ley de Privacidad y Derechos Educativos de la Familia (FERPA*), privacidad, falta de consentimiento informado, seguridad de datos, derechos de propiedad intelectual y conformidad con las leyes de registros públicos y retención. Las personas que graben o transcriban reuniones virtuales organizadas por el Distrito sin autorización pueden ser expulsadas de la reunión. Esta política se aplicará de acuerdo con las leyes estatales y federales de discapacidad. Si la reunión virtual es organizada por una organización o entidad que no pertenece al Distrito, usted puede asistir y participar incluso si se está transcribiendo o grabando.
6. Una cuenta cancelada no conservará el correo electrónico.
7. Los administradores del sistema se reservan el derecho de cancelar el acceso a los recursos de la red informática del Distrito si se infringe esta AUP mientras se utilizan las funciones de chat en tiempo real, incluidas las videoconferencias.

J. Uso Personal Incidental de los Recursos Tecnológicos

1. Los recursos tecnológicos pueden ser utilizados por el personal del Distrito para fines personales siempre que el

uso no interfiera con la capacidad del Distrito para llevar a cabo los asuntos del Distrito, no interfiera con los deberes del empleado, no exponga al Distrito a mayores costos o riesgos, y no infrinja los términos de esta Política de Uso Aceptable.

K. Seguridad y Privacidad

1. Los usuarios deben proteger toda la información confidencial y de identificación personal (PII*) que encuentren al utilizar los recursos de red del Distrito. El manejo de datos, el almacenamiento y la transmisión de dicha información deben cumplir con las políticas del Distrito y los estándares de protección de datos. La divulgación, el acceso o la transferencia no autorizados de PII están estrictamente prohibidos.
2. El acceso remoto a los recursos del Distrito solo se permite a través de métodos seguros aprobados por el Distrito, como las Redes Privadas Virtuales (VPN*) y las tecnologías de Servicio de Acceso Seguro Edge (SASE*) aprobadas por el Distrito.
3. Los usuarios no pueden instalar o utilizar aplicaciones no autorizadas o no aprobadas que puedan introducir vulnerabilidades de seguridad.
4. Los usuarios deben asegurarse de que todas las aplicaciones aprobadas por el Distrito estén actualizadas a las últimas versiones para mitigar los riesgos de seguridad.
5. El Distrito se reserva el derecho a monitorear la actividad de la red, incluido el uso de internet y el acceso a archivos, para garantizar el cumplimiento de esta AUP y proteger los recursos del Distrito. Los usuarios deben comprender que no hay expectativas de privacidad al utilizar los recursos de red del Distrito.

6. El intercambio de datos con terceros requiere autorización previa y debe cumplir con las regulaciones de protección de datos del Distrito, incluida la FERPA. Cualquier acceso de proveedor o de terceros a los recursos del Distrito debe cumplir con las políticas de seguridad del Distrito, los estándares y los acuerdos de intercambio de datos establecidos.
7. Todos los intercambios de datos con proveedores externos deben estar documentados, aprobados y sujetos a revisión para el cumplimiento de la seguridad.
8. Todos los usuarios deben completar una capacitación de concientización sobre ciberseguridad, que cubra temas como fraude electrónico, uso seguro de internet, seguridad de contraseñas y reconocimiento de ataques de ingeniería social.
9. La información confidencial debe encriptarse tanto en tránsito como en reposo. Se requiere que los usuarios utilicen métodos de encriptación aprobados por el Distrito cuando manejen, almacenen o transmitan datos confidenciales.

L. Uso Justo y Ético de Inteligencia Artificial (AI*)

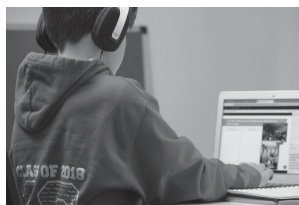
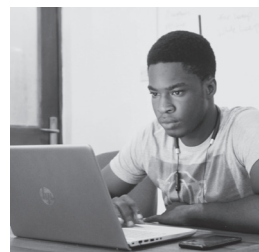
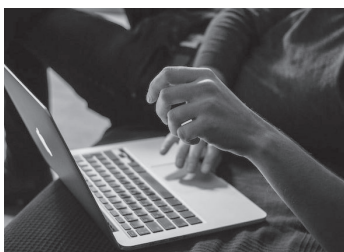
1. Las herramientas y recursos de AI proporcionados por el Distrito están destinados a fines educativos y deben usarse de manera justa, ética e imparcial.
2. Se espera que los usuarios de herramientas de AI evalúen críticamente las fuentes y los resultados de los contenidos generados por AI y que eviten perpetuar inclinaciones o estereotipos perjudiciales.
3. El uso de herramientas de AI generativa proporcionadas por el Distrito debe alinearse con las políticas del Distrito, y los usuarios deben abstenerse de ingresar información confidencial en herramientas de AI externas.

4. Se prohíbe a los usuarios utilizar contenido generado por AI que incluya información de identificación personal sin cumplir con las políticas de privacidad de datos del Distrito y las pautas regulatorias pertinentes.
5. Está estrictamente prohibido el uso de herramientas de AI para difundir información falsa o errónea.
6. Los usuarios tienen prohibido utilizar las herramientas de AI para crear contenido engañoso, erróneo o falsificado, incluyendo falsificación profunda, plagio, automatización no autorizada de las operaciones del Distrito o cualquier contenido que infrinja las normas éticas o legales.

El uso de los recursos tecnológicos de la red informática será consistente con todas las políticas y regulaciones del Distrito, incluyendo, pero no limitado a, la Regulacion 3990 y Regulacion 3991.

Los estudiantes recibirán acceso a los recursos de la red del Distrito a menos que un padre/tutor indique explícitamente que el estudiante no debe tener acceso a los recursos de la red del Distrito. Todo el personal recibirá acceso a los recursos de la red del Distrito al momento de la contratación.

Esta política se alinea con las políticas y regulaciones del Distrito, así como con las leyes federales y estatales aplicables, incluyendo, pero no limitado a, los requisitos de protección de datos de FERPA, CIPA, la Ley de Protección de la Privacidad en Línea de Menores (COPPA*) y los Estatutos Revisados de Nevada (NRS*).



La tecnología habilita al aprendiente para el viaje de su vida.

*Por sus siglas en inglés.



División de Servicios de Tecnología & Sistemas de Informática

Distrito Escolar del Condado de Clark
4212 Eucalyptus Avenue
Las Vegas, NV 89121

Teléfono: 702-799-3321 Fax 702-799-6143
www.ccsd.net