

RED OAK ISD

2024-2025

APÉNDICE A

**Política de Seguridad en el
Internet y Uso Aceptable de
Recursos de Tecnología**

Distrito Escolar Independiente de Red Oak

Procedimientos para el uso seguro de Internet

Introducción

Es la política del distrito escolar independiente Red Oak ("ROISD"): (a) prevenir el acceso de los usuarios sobre su red informática o transmisión de material inadecuado a través de Internet, correo electrónico u otras formas de comunicación electrónica directa; (b) prevenir el acceso no autorizado y otras actividades ilegales en línea; (c) prevenir la divulgación en línea no autorizada, uso o difusión de información de identificación personal de menores de edad; y (d) cumplir con la ley de protección de Internet de los niños ("CIPA"). Es el objetivo de esta política no solo prevenir y proteger, sino educar a los empleados, estudiantes, padres y la comunidad de ROISD en seguridad en Internet. Las directrices de la CIPA para una política de seguridad de Internet también se han incorporado por ROISD en su política de uso aceptable de tecnología y recursos.

La ley de protección de Internet de los niños, promulgada el 21 de diciembre de 2000, requiere que los receptores de fondos federales cumplan con ciertos requisitos de filtración y política de Internet. Las escuelas y bibliotecas que reciben fondos para acceso a Internet o servicios de conexión interna deben cumplir también con las políticas de seguridad de Internet de la ley de los niños del vecindario de protección de Internet ("NCIPA") que se ocupa de las cuestiones más amplias de mensajes electrónicos, divulgación de información personal de menores de edad y de actividades ilegales en línea. Además, el Proyecto de Ley No. 18 de la Cámara de Representantes de Texas, la Ley de Protección de los Niños en Línea a través del Empoderamiento de los Padres (SCOPE), promulgada el 13 de junio de 2023, requiere que los proveedores de servicios digitales cubiertos brinden a los menores ciertas protecciones de datos, eviten que los menores accedan a contenido dañino y brinden a los padres herramientas para administrar el uso del servicio por parte de sus hijos.

Esta política pretende ser leída junto con la política de uso aceptable de recursos de tecnología de ROISD. Todas las limitaciones y las sanciones establecidas en la política de uso aceptable de tecnología y recursos se consideran incorporadas a esta política. Los términos utilizados en esta política que también aparecen en la ley de protección de los niños en Internet tienen los significados definidos en la ley de protección de los niños en Internet.

Cumplimiento de los requisitos de CIPA:

Medidas de protección de tecnología

Una medida de protección es una tecnología específica que bloquea o filtra el acceso a Internet. Debe proteger contra el acceso de adultos y menores a representaciones visuales que son obscenas, implican pornografía infantil o son perjudiciales para los menores de edad. ROISD utiliza un sofisticado sistema ubicado en el nivel del firewall para que todos los equipos estén sujetos a filtrado que cumple con CIPA y NCIPA de filtrado de contenidos.

Acceso a material inadecuado

A los fines prácticos, las medidas de protección tecnológica (o "Filtros de Internet") se utilizarán para bloquear o filtrar Internet y otras formas de comunicaciones electrónicas y el acceso a información inadecuada. Específicamente, como requiere por CIPA y la Ley SCOPE, el bloqueo se aplicará a las representaciones visuales y textuales de material considerado obsceno o pornografía infantil, o cualquier

material considerado perjudicial para menores. Sujeto a aprobación administrativa, las Medidas de Protección Tecnológica pueden desactivarse o, en el caso de menores, minimizarse solo para investigación de buena fe u otros fines legales. Cualquier intento de eludir, derrotar o eludir las Medidas de Protección Tecnológica es punible como una violación de esta política y de la Política de Uso Aceptable de Recursos Tecnológicos.

Uso inadecuado de la red

A los fines prácticos, se tomarán medidas para promover la protección y la seguridad de los usuarios de la red de computadoras en línea ROISD al usar el correo electrónico, salas de chat, blogs, mensajería instantánea, conversaciones en línea y otras formas de comunicación electrónica directa. Sin perjuicio de lo anterior, el acceso a los medios de comunicación está limitado estrictamente por la política de uso aceptable de recursos de tecnología. Específicamente, como requiere por CIPA y la Ley SCOPE, la prevención de uso inadecuado de la red incluye: (a) acceso no autorizado, incluyendo el llamado "hacking" y otras actividades ilegales; y (b) divulgación, uso y difusión no autorizados de la información de identificación personal con respecto a los menores de edad.

Supervisión y Monitoreo

Será responsabilidad de todos los empleados profesionales (personal administrativo y pedagógico) de ROISD supervisar y monitorear el uso de computadoras del distrito escolar, red informática y acceso a Internet según esta política, la política de uso aceptable de recursos de tecnología y CIPA y Ley SCOPE. De acuerdo con la Ley SCOPE, ROISD ha asegurado un software de filtrado de Internet que bloquea el contenido inapropiado y alerta a los administradores si los estudiantes intentan acceder a dicho contenido. La administración de la escuela notificará a los padres sobre alertas de uso inapropiado. Los procedimientos para la desactivación o de lo contrario modificar las medidas de protección de la tecnología serán responsabilidad del Director de tecnología o representantes designados.

Educación

ROISD defenderá y educará a los empleados, estudiantes, padres y la comunidad de ROISD sobre seguridad en Internet e "intimidación cibernética". De acuerdo con la Ley SCOPE, la educación de los padres se prestará a través de medios tales como capacitación de desarrollo profesional y materiales para empleados, presentaciones de PTA, la Universidad de Padres y el sitio web del distrito escolar.

Intimidación cibernética

La política de uso aceptable de recursos de tecnología incluye disposiciones para prohibir y establecer las sanciones por conducta inadecuada y opresiva, incluyendo acoso cibernético. ROISD es un lugar de tolerancia y buenos modales.

- Los estudiantes no pueden usar la red o las instalaciones del equipo de ROISD para transmitir odio por correo, declaraciones difamatorias, declaraciones que pretenden herir o humillar a otros por la divulgación de información personal (ya sea verdadero o falso), ataques personales a los demás, y declaraciones expresando animadversión hacia una persona o grupo por razón de raza, color, religión, origen nacional, género, orientación sexual o discapacidad.
- Los usuarios de la red no pueden usar lenguaje vulgar, despectivo u obsceno.
- Los usuarios de la red no pueden enviar mensajes anónimos inapropiados o forjar otros mensajes o correo electrónico.

- Las computadoras y instalaciones de red de ROISD no pueden utilizarse para ninguna actividad, o para la transmisión de ningún material, que viole leyes locales o del estado de Texas o Estados Unidos. Esto incluye, entre otros, cualquier amenaza o acto de intimidación o acoso contra otra persona.

Restricciones de tiempo

De acuerdo con la Ley SCOPE, Red Oak ISD ha implementado restricciones de tiempo en los dispositivos de los estudiantes. Todos los dispositivos de los estudiantes de primaria permanecerán en el campus. Dentro de la jornada educativa, los maestros utilizarán una combinación de estrategias de instrucción digitales y no digitales. Además, en el caso de una situación de seguridad cibernética, es posible que se requiera que ROISD deshabilite los dispositivos de los estudiantes para mitigar la amenaza hasta que se determine una solución.

Privacidad de datos

Red Oak ISD adoptará aplicaciones de software que recopilen solo los datos estrictamente necesarios para fines educativos. Los recursos y las solicitudes en línea se aprobarán a través de un proceso distrital semestral. Una lista de solicitudes aprobadas está disponible en el sitio web de Tecnología Educativa de ROISD.

Distrito Escolar Independiente de Red Oak

Política de uso aceptable de recursos de tecnología

Introducción

El Distrito Escolar Independiente de Red Oak pone una variedad de tecnologías de información y comunicación disponibles para los estudiantes, empleados y otros usuarios autorizados para mejorar el ambiente de aprendizaje y promover la excelencia educativa. Estas tecnologías, cuando se usan correctamente, proporcionarán beneficios educativos a los estudiantes y empleados a través de intercambio de recursos, la innovación y la comunicación. El propósito de esta política de uso aceptable es educar a los estudiantes del distrito, empleados y usuarios autorizados de las normas y estándares de comportamiento a seguir al utilizar los recursos de tecnología del distrito, así como las consecuencias por no conocer las reglas y normas. El distrito cree firmemente que la información valiosa y la interacción disponible mediante el uso de los recursos de tecnología del distrito es mayor que la posibilidad de que los usuarios interactúen con el material de forma no coherente con los objetivos educativos del distrito.

Revisión obligatoria

Para educar a los empleados del distrito, estudiantes y usuarios autorizados en el correcto uso de los recursos de la tecnología y la conducta, todos los usuarios deberán revisar estas pautas al inicio del año escolar. Todos los empleados del distrito estarán obligados a reconocer la recepción y comprensión de todas las regulaciones administrativas que rigen el uso del sistema y deberán acordar por escrito permitir la supervisión de su uso y cumplir con estas regulaciones y directrices. El estudiante y el padre o tutor legal deben acusar recibo y comprensión de la política de uso aceptable como parte de su revisión del Plan de manejo de disciplina y el manual del Código de Conducta Estudiantil. Todos los recibos se mantendrán en el archivo de la oficina del director o del supervisor departamental. Los empleados que supervisen estudiantes que utilizan el sistema del distrito deben proporcionar capacitación haciendo hincapié en su uso apropiado.

Recursos de tecnología del distrito

Los recursos tecnológicos del distrito se refieren a cualquier configuración de hardware y software que funciona y es proporcionado por Red Oak ISD, incluyendo sistemas informáticos electrónicos, sistemas de gestión de datos e infraestructura de comunicación. El sistema incluye, entre otros:

- Teléfonos, teléfonos celulares, buscapersonas y servicios de correo de voz;
- Red de comunicaciones de datos, Wi-Fi;
- Cuentas de correo electrónico;
- Impresoras, copiadoras, máquinas de fax;
- Servidores;
- Hardware y periféricos;
- Software incluido, software de sistema operativo y software de aplicación; I
- Información digitalizada incluyendo texto almacenado, archivos de datos, correo electrónico, imágenes digitales y archivos de audio;
- Bases de datos o herramientas a las que se accede internamente;
- Bases de datos o herramientas a las que se accede externamente (como Internet); y
- Tecnologías adicionales que están disponibles.

Uso aceptable

Los recursos de tecnología se utilizarán para mejorar el aprendizaje y la enseñanza coherente con los objetivos educativos del distrito. El Distrito requiere uso legal, ético y apropiado de todos los recursos de tecnología.

Acceso a recursos tecnológicos. La red y el acceso a Internet se proporcionan a todos los docentes del distrito y personal. A los estudiantes se les permitirá utilizar la red local con permiso del campus, pero solo pueden usar el Internet con permiso de los padres. Todo acceso a Internet será monitoreado por el personal del distrito. Todos los usuarios que no sean empleados ni estudiantes deben obtener la aprobación del director de tecnología o su designado individual para acceder al sistema del distrito.

El acceso al sistema de comunicaciones electrónicas del distrito, incluyendo el Internet, se facilitará a los estudiantes y empleados principalmente con fines de instrucción y administrativos y de conformidad con las disposiciones administrativas. El uso personal limitado se permite si no impone costo tangible para el distrito, demasiada carga al ordenador o los recursos de la red del distrito y no tiene ningún efecto adverso en el desempeño de un empleado en el trabajo o en el rendimiento académico de un estudiante.

Privilegio. El acceso a los recursos de tecnología del distrito es un privilegio, no un derecho. Como tal, el acceso puede ser negado para cualquier persona por cualquier razón a criterio del distrito.

Contenido-información suministrada por terceros. Los usuarios del sistema y los padres de estudiantes con acceso al sistema del distrito deben ser conscientes de que el uso del sistema puede proporcionar acceso a otros sistemas de comunicaciones electrónicas en la red electrónica mundial que puede contener material inexacto u ofensivo. Un usuario que obtiene acceso a dicho material se espera que deje el acceso tan rápidamente como sea posible e informe el incidente al miembro del personal de supervisión.

Seguridad

El sistema de seguridad es una prioridad y la responsabilidad de todos los usuarios del sistema.

Reportando el problema de seguridad. Si se identifica el conocimiento de material inadecuado o un problema de seguridad en los recursos de tecnología del distrito, el usuario debe notificar inmediatamente a *Help Desk* o a un miembro del personal de supervisores del distrito. El problema de seguridad no debe ser compartido con otros.

Cuentas. Personal, estudiantes y otros usuarios autorizados que se asignan a cuentas individuales se harán responsables de toda actividad registrada en esa cuenta. Cuando cualquier usuario en una cuenta emitida por el distrito viola la política del distrito, el distrito atribuye esta conducta a la persona asignada a la cuenta. Permitir que un tercero utilice una cuenta del Distrito no será una defensa a la disciplina del estudiante o empleado. Los usuarios del sistema no pueden utilizar la cuenta de otra persona.

Contraseñas. Las contraseñas son la principal forma en que los usuarios son autenticados y se les permite el uso de recursos de computación del distrito. Los usuarios del sistema están obligados a mantener la confidencialidad de la contraseña no compartiendo su contraseña con otros y reconociendo que, si lo hacen, serán responsables de sus acciones así como de los demás a quienes hayan dado acceso.

Filtrado. Los sitios accesibles a través de recursos de tecnología del distrito pueden contener material ilegal, difamatorio, inexacto o controvertido. Cada equipo del distrito con acceso a Internet tiene software de filtrado que bloquea el acceso a representaciones visuales obscenas, pornográficas, inadecuadas

para los estudiantes o perjudiciales para los menores de edad, según lo definido por la ley federal de protección de los niños en Internet y la Ley SCOPE. El distrito hace todo lo posible para limitar el acceso a material censurable; sin embargo, controlar todos estos materiales en Internet es imposible, incluso con filtros implementados. Con acceso global a los equipos y personas, existe el riesgo de que los estudiantes puedan acceder a material que puede ser inadecuado y no de valor educativo en la escuela. La conexión a Internet de Red Oak es el único sistema para ser utilizado en las escuelas. No pueden utilizarse cuentas de Internet comerciales.

Privacidad de datos. Con el fin de proporcionar a los estudiantes acceso a las solicitudes y recursos en línea, el distrito compartirá solo los datos estrictamente necesarios para fines educativos. El distrito revisará semestralmente los acuerdos de privacidad de datos y se asegurará de que se tomen medidas para compartir de manera segura la información requerida. La información de identificación personal del estudiante solo se comparte con los recursos aprobados por el distrito. Se anima a los padres a revisar la lista de recursos aprobados en el sitio web de Tecnología Educativa del distrito. Además, se prohíben estrictamente las aplicaciones de software no aprobadas que realicen evaluaciones no educativas o recopilen información sobre los estudiantes.

Monitoreo

Todo el uso del sistema del distrito está sujeto a supervisión por personal designado en cualquier momento para asegurar el uso apropiado. Los usuarios deben tratar el sistema de la computadora como un sistema de archivo compartido o común con la expectativa de que los archivos electrónicos enviados, recibidos o almacenados en cualquier lugar en el sistema informático estarán disponibles para examen por cualquier representante autorizado del distrito y pueden estar sujetos a divulgación pública bajo la ley de información pública de Texas. Los usuarios del sistema no deben utilizar el sistema informático para enviar, recibir o almacenar cualquier información, incluyendo mensajes de correo electrónico que consideren confidencial o personal y deseen mantener en privado. El distrito se reserva el derecho a acceder, revisar, copiar, eliminar, modificar o divulgar dicha información para cualquier propósito. El personal del distrito supervisará y examinará todos los usuarios de los sistemas del distrito para asegurar un uso adecuado y ético.

Uso inadecuado

El uso inadecuado incluye, entre otros, aquellos usos que violen la ley, que se nombran específicamente como infracciones en este documento, que violan las reglas de etiqueta de la red, o que dificultan la integridad o la seguridad de este o cualquiera de los componentes que están conectado a la computadora/red/Internet. Las siguientes acciones se consideran usos inadecuados y están prohibidas:

Se prohíbe la transmisión de cualquier material que violación cualquier ley federal o estatal. Esto incluye, pero no se limita a:

- material con derechos de autor;
- material plagiado;
- material amenazador, acosador, difamatorio u obsceno;
- material protegido por secreto comercial.

Intimidación. Cualquier uso de recursos de tecnología del distrito para amenazar, acosar, difamar, humillar, avergonzar o de otra manera atacar a una persona está prohibido.

Propiedad intelectual. Maestros, personal y estudiantes siempre deben respetar los derechos de autor y marcas registradas de terceros y sus reclamos de propiedad en imágenes, texto, material de video y

audio, software, información e invenciones. No se permite la copia, uso o transferencia de otros materiales sin la autorización correspondiente.

Suplantación/plagio. Se prohíbe alterar o copiar fraudulentamente documentos o archivos creados por otra persona. Se prohíbe crear fraudulentamente un documento o comunicación y atribuirlos a otra persona. Asumir la identidad de otra persona está prohibido.

Violaciones de datos/archivo. Borrar, examinar, copiar o modificar archivos o datos pertenecientes a otros usuarios sin su permiso o autorización del distrito está prohibido.

Hackeo/elusión. Está prohibido cualquier intento de hackear o burlar firewalls del distrito, filtros o sistema de seguridad. El acceso no autorizado a sistemas del distrito y datos está prohibido.

Transmitir información confidencial. Maestros, personal y estudiantes no pueden redistribuir o reenviar información confidencial (es decir, registros educativos, información, registros de personal, etc.) sin la debida autorización. La información confidencial no debe ser transmitida, redistribuida o reenviada a personas afuera que no están expresamente autorizadas para recibir la información. Está prohibido revelar información personal como direcciones o números de teléfono de los usuarios u otros.

Modificación de la computadora. Está prohibido modificar o cambiar la configuración del equipo o configuraciones internas o externas sin el permiso adecuado. Está prohibido agregar o quitar cualquier software o hardware sin el permiso escrito del Director de tecnología o su designado. La alteración o robo de componentes de sistemas del distrito puede considerarse actividad penal bajo las leyes federales y estatales aplicables.

Uso comercial. El uso del sistema para cualquier tipo de actividad de generación de ingresos está prohibido. Se prohíbe la publicidad de la venta de productos, ya sea comercial o personal.

Mercadeo de organizaciones que no son ROISD. Queda prohibido el uso del sistema para la promoción de actividades o eventos para individuos u organizaciones no afiliadas directamente o aprobada por el distrito.

Cabildeo político. En concordancia con las leyes de ética estatal, los recursos y equipo del distrito, incluyendo, entre otros, correo electrónico, no deben utilizarse para llevar a cabo ninguna actividad política, incluyendo la publicidad o el cabildeo político.

Vandalismo/travesura. Cualquier intento malicioso de dañar o destruir equipo del distrito, materiales o datos; o el intento malicioso de dañar o destruir datos de otro usuario del sistema del distrito, o de cualquiera de las agencias o de otras redes a las que el distrito tiene acceso está prohibido. Está prohibido cualquier intento deliberado para degradar o alterar el rendimiento del sistema.

Consecuencias de políticas inadecuadas

Las violaciones de los procedimientos de ROISD pueden resultar en la suspensión del acceso y terminación de los privilegios, otra acción disciplinaria consistente con las políticas de la Junta, el código de conducta estudiantil y leyes estatales o federales. Esto también puede requerir restitución de costos asociados con los costos de restauración, hardware o software del sistema. El distrito cooperará completamente con los funcionarios locales, estatales o federales en cualquier investigación sobre o en relación al mal uso de los recursos de tecnología del distrito.

Comunicación electrónica

Comunicación electrónica abarca todas las comunicaciones enviadas a través de dispositivos tecnológicos. Puede incluir correo electrónico, páginas web, documentos electrónicos, imágenes electrónicas, sonido electrónico, video electrónico y medios sociales como blogs, wikis, foros y tableros

de mensajes. Todo el personal, estudiantes, padres y usuarios autorizados deben ser conscientes de su responsabilidad de utilizar estos recursos de una manera positiva. El distrito anima el uso de la comunicación electrónica para mejorar el ambiente de aprendizaje coherente con metas educativas del distrito.

Los medios de comunicación social. Estudiantes y empleados podrán participar en los medios sociales, entornos de aprendizaje (tales como, entre otros, blogs, foros, RSS feeds, wikis y foros) dentro de una oportunidad de aprendizaje segura aprobada por el distrito, protegida y con base en el plan de estudios.

Correo electrónico. Correo electrónico (e-mail) es una de las herramientas de comunicación más usadas en el distrito. Todos los maestros y personal reciben cuentas de correo electrónico para las necesidades de instrucción y administrativas. Los usuarios deben revisar el correo electrónico frecuentemente, eliminar mensajes no deseados inmediatamente. Los archivos adjuntos de correo electrónico están limitados a 15 MB o menor.

Representación percibida. Los usuarios deben ser conscientes de que las comunicaciones electrónicas relacionadas con la escuela pueden causar que algunos destinatarios u otros lectores asuman que los comentarios del usuario representan al distrito o escuela, aunque esa no sea la intención del usuario.

Privacidad. La comunicación electrónica no debe considerarse privada. Los usuarios deben ser conscientes de que cualquier comunicación electrónica puede convertirse en información pública, disponible para verla por cualquier persona o entidad. La información confidencial, como direcciones o números de teléfono, no debe ser divulgada en comunicaciones electrónicas sin la autorización de la persona involucrada.

Lenguaje inapropiado. Está prohibido usar lenguaje obsceno, profano, lascivo, vulgar, grosero, provocador, amenazante o irrespetuoso en comunicaciones electrónicas distribuidas a través de recursos de tecnología del distrito. Enviar mensajes que pueden causar peligro o perturbación, ataques personales, incluyendo ataques perjudiciales o discriminatorios está prohibido.

Falsificación. Falsificación o intento de falsificación de mensajes de correo electrónico u otras comunicaciones electrónicas están prohibidos y penados por la ley. Intentar leer, borrar, copiar o modificar las comunicaciones de otros usuarios del sistema, la interferencia deliberada con la capacidad de otros usuarios del sistema para utilizar la comunicación electrónica o el uso de ID de usuario de otra persona o la contraseña están prohibidos.

Correo basura o Cartas en cadena. Generalmente, los usuarios deben abstenerse de reenviar e-mails o comunicaciones que no se refieren a los propósitos educativos del distrito. Las cartas en cadena u otros mensajes de correo electrónico para la expedición o distribución a otros están prohibidos. También está prohibido crear o distribuir mensajes innecesarios a personas (spamming).

Uso de recursos. Los usuarios deben limitar las comunicaciones electrónicas para las funciones de instrucción y administrativas.

Cuentas de correo electrónico del estudiante. Las cuentas de correo electrónico de estudiante pueden ser proporcionadas directamente por el distrito o a través del sistema de gestión de contenidos de un curso en línea aprobado. Según sea el caso y con autorización por escrito del personal designado del distrito en el Departamento de tecnología, se concederán cuentas de correo electrónico de proyecto para determinadas actividades educativas. Los estudiantes que tienen acceso a una cuenta de correo electrónico deben acatar los lineamientos establecidos para la comunicación electrónica. Los

estudiantes tienen prohibidos acceder a cuentas personales de comunicación electrónica (correo electrónico, Facebook, Twitter, etc.) usando el sistema del distrito.

Presentación de la información de los estudiantes en los sitios web del distrito. Las siguientes condiciones se aplican a la visualización de información en sitios web del distrito. Un contribuyente de contenido que a sabiendas infringe (o promueve la violación de) cualquier porción de estas directrices estará sujeto a acción disciplinaria conforme a las políticas del distrito.

Proyectos, escrituras o arte creados por el estudiante están permitidos en los sitios web del campus/distrito si se ha obtenido el consentimiento de padres/estudiante adecuado.

Fotografías o nombres de estudiantes se permiten si la información de directorio especificada para el estudiante lo permite.

Todas las fotografías de estudiantes o trabajos de estudiantes pueden mostrarse sin el nombre del estudiante. No se permite ninguna otra información personal del estudiante, incluyendo, entre otros, nombre, dirección de correo electrónico, número de teléfono, dirección o fecha de nacimiento.

Renuncia de responsabilidad

El sistema del distrito se proporciona sobre una base "tal cual, según esté disponible". El distrito no hace garantías, expresas o implícitas, incluyendo, entre otras, aquellas de comerciabilidad e idoneidad para un propósito particular con respecto a cualquier servicio proporcionado por el sistema y cualquier información o software contenido en él. El distrito no garantiza que las funciones o servicios realizados o que la información o software contenidos en el sistema cumplirán con los requisitos del usuario del sistema o que el sistema será ininterrumpido o libre de errores o los defectos serán corregidos.

Opiniones, consejos, servicios y toda otra información expresada por los usuarios del sistema, proveedores de información, proveedores de servicios u otras personas en el sistema son los de los proveedores y no del distrito. El distrito cooperará completamente con los funcionarios locales, estatales o federales en cualquier investigación sobre o en relación al mal uso de comunicación electrónica del distrito.

Cláusula elástica. La escuela y la administración se reservan el derecho a establecer reglas justas y razonables para circunstancias que puedan surgir que requieren acciones que no están cubiertos por estas directrices. En todos los casos, las reglas, regulaciones y posibles consecuencias serán tan consistentes como sea posible con reglas previamente establecidas, normas y consecuencias para incidentes similares.

Los asuntos omitidos de estas directrices no deberían interpretarse como una limitación al alcance de la responsabilidad del distrito y, por lo tanto, la autoridad del distrito en relación con cualquier tipo de infracción que no sea en el mejor interés de la seguridad y el bienestar de los estudiantes.

Estas normas y políticas se aplican a cualquier estudiante que está en propiedad de la escuela, que asista a la escuela o cualquier actividad patrocinada por la escuela, o cuya conducta en cualquier momento o lugar directamente interfiere con las operaciones, la disciplina o el bienestar general del distrito, escuelas, estudiantes y personal.

Más información

Estas pautas fueron desarrolladas en virtud de la Junta Directiva CQ(LOCAL). Puede encontrar más información en las siguientes ubicaciones:

- [Reglamento de la mesa directiva](#)

- [Código de Conducta del Estudiante](#)
- [Manual del empleado](#)