I-18: Procedimientos administrativos Uso aceptable del Internet, computadoras y recursos en línea por parte de los estudiantes

SALT LAKE CITY SCHOOL DISTRICT
Your Best Choice

REFERENCIAS

Política I-18 del Consejo:

DEFINICIONES

Dispositivos electrónicos: Cualquier dispositivo utilizado para la comunicación por medio de audio, vídeo o texto, o cualquier otro tipo de computadora o instrumento similar, incluyendo:

A. un teléfono inteligente;
B. un reloj inteligente o electrónico;
C. una tableta; o
D. un dispositivo de realidad virtual

PROCEDIMIENTOS DE IMPLEMENTACIÓN

I. Autoridad

A. El distrito tiene el derecho, y en algunos casos la obligación legal, de poner restricciones al uso y acceso de los estudiantes a los dispositivos electrónicos y a los sistemas de computadoras, redes de computadoras, herramientas y dispositivos adaptados al distrito, aplicaciones de software, correo electrónico e Internet (llamados colectivamente "recursos electrónicos").

B. En general, todos los estudiantes son responsables del uso responsable, ético y legal de los recursos electrónicos del distrito. Al usar estos recursos, los estudiantes deben cumplir estos procedimientos administrativos, así como la Politica S-3 del Consejo: Comportamiento y disciplina de los estudiantes

II. Acceso a los recursos electrónicos del distrito

A. A través del proceso de inscripción, los padres y los estudiantes atestiguarán que han leído y entendido estos procedimientos administrativos y la política de la junta que los acompaña ("Contrato de Uso Responsable").
   1. Los padres pueden cancelar el acceso de su estudiante de acuerdo con la Sección VI.C.

B. Como mínimo, los maestros revisarán estos procedimientos administrativos y otras reglas y regulaciones aplicables con los estudiantes de forma anual, pero se les anima a los maestros a discutir con los estudiantes las pautas de uso apropiado de forma regular cuando usen los recursos electrónicos del distrito.

C. Después de inscribirse en el distrito, todos los estudiantes recibirán una contraseña para acceder a los recursos electrónicos del distrito.

III. Privilegios

A. El uso de los recursos electrónicos del distrito es un privilegio, no un derecho. El uso inapropiado puede dar lugar a una pérdida de los privilegios de red, acciones disciplinarias o la denuncia ante las autoridades. Los administradores del sistema tienen la autoridad de cerrar una cuenta en cualquier momento.
   1. Un administrador o miembro del profesorado puede solicitar al administrador del sistema que niegue, revoque o suspenda el acceso de un usuario específico y/o sus cuentas de usuario.

B. Al acceder a los recursos de la red del distrito, los estudiantes reconocen que han leído, entendido y están de acuerdo con cumplir con las disposiciones de las Políticas del Consejo I-18 y S-3, y los procedimientos administrativos que las acompañan.

IV. Uso aceptable

A. El uso de los recursos electrónicos del distrito por parte de un estudiante será únicamente para fines educativos, lo que incluye el acceso y el intercambio de información con los maestros y otros estudiantes, el almacenamiento de archivos, la realización de investigaciones y la colaboración en proyectos con otros.
   1. En algunos casos, los maestros pueden ordenar a los estudiantes que utilicen los recursos electrónicos del distrito junto con su plan de estudios, una evaluación o un programa de apoyo a la conducta.

B. Se espera que los estudiantes cumplan con las reglas generalmente aceptadas de la etiqueta de la red. Esto incluye, pero no se limita a, lo siguiente:
   1. Sea amable.
   2. No sea abusivo en sus mensajes a otros.
   3. Use lenguaje apropiado.

4. Si una persona le pide que deje de mandar mensajes, la persona que los envía tiene que parar.

V. Cuidado de los dispositivos electrónicos del distrito

A. Los dispositivos electrónicos utilizados por los estudiantes se utilizarán principalmente para fines educativos que estén directamente relacionados con un proyecto o tarea escolar, a menos que lo autorice la administración del edificio. El uso personal de los dispositivos electrónicos del distrito por parte de los estudiantes solo puede ser incidental y no puede interrumpir el ambiente de aprendizaje.

B. Los estudiantes son responsables del cuidado apropiado de cada dispositivo electrónico del distrito que utilizan. Los estudiantes y sus padres pueden ser responsables de los costos asociados con la reparación de las computadoras dañadas. Los costos de reparación de computadoras pueden exceder los $700. Si un estudiante o padre no puede pagar las reparaciones, se pueden establecer formas alternativas de restitución con la administración del edificio.

VI. Usos no permitidos

Están prohibidos los siguientes usos de los recursos electrónicos del distrito:

A. Uso ilegal: cualquier uso que viole o apoye la violación de las leyes federales, estatales o locales, la política de la junta, las reglas de la escuela y/o el código de conducta estudiantil (incluyendo cualquier forma de intimidación, humillación y acoso); el uso de materiales con derechos de autor o materiales protegidos por secretos comerciales sin la autorización apropiada; cualquier uso que viole los acuerdos de licencia de software; y cualquier uso que constituya plagio.

B. Vandalismo y/o robo: cualquier intento deliberado de dañar el hardware, software o información residente en la red del distrito o cualquier otro sistema de computación conectado a través del Internet; violar, o intentar violar, la integridad de cuentas, archivos o programas privados; infectar deliberadamente una computadora con un virus; hackear computadoras usando cualquier método; interferir con el desempeño de la computadora o de la red; interferir con la capacidad de otra persona para usar el equipo y sistemas; destruir información.

C. Uso comercial: cualquier uso para propósitos o actividades comerciales que resulten en una ganancia financiera personal, incluyendo anuncios y solicitaciones de productos.

D. Comportamiento ofensivo o acosador: cualquier uso de material, ya sea visual o textual, que pueda ser considerado profano, vulgar, pornográfico, indecente, abusivo, amenazante, obsceno o sexualmente explícito; distribución de declaraciones despectivas o acosadoras, incluyendo aquellas que puedan incitar a la violencia o que se basen en la raza, el color, el embarazo, la identidad de género, la información genética, el origen nacional, el sexo, la orientación sexual, la edad, la discapacidad o las creencias políticas o religiosas; publicación de mensajes anónimos.

E. Uso religioso o político: cualquier uso para un propósito religioso o político, incluyendo el proselitismo religioso y la presión para las elecciones del cuerpo estudiantil.

F. Violaciones de seguridad: usar una cuenta que no sea la suya; acceder o intentar acceder a cuentas, sitios, servidores, archivos, bases de datos u otros sistemas para los cuales un estudiante no está autorizado (por ejemplo, "piratería informática" o uso de "spyware"); propagar virus informáticos; degradar o interrumpir el equipo de red, el software o el rendimiento del sistema; ejecutar aplicaciones o archivos que creen un riesgo de seguridad; cualquier otra acción que amenace la seguridad de los recursos electrónicos del distrito.

G. Compartir o acceder a información confidencial: transmitir información confidencial sobre otros individuos; violar la privacidad de otros al leer o publicar correo electrónico u otras comunicaciones privadas sin obtener el consentimiento apropiado; proporcionar direcciones personales, números de teléfono o información financiera en cualquier comunicación de la red, ya sea que esa información pertenezca al estudiante o a cualquier otro individuo, a menos que esté relacionada con un objetivo educativo apropiado en el plan de estudios.

H. Usos innecesarios: descargar o transmitir archivos de audio o vídeo, o cualquier otro archivo que no esté directamente relacionado con el plan de estudios del curso; jugar a juegos no educativos en Internet; acceder o utilizar servicios en Internet que impongan una tarifa al estudiante.

I. Manipulación: cualquier intento de pasar por alto la seguridad del estado, del distrito o de la escuela; intentar desactivar o pasar por alto el software de bloqueo/filtrado de Internet del distrito sin autorización; añadir, modificar, reparar, eliminar, reconfigurar o manipular cualquier dispositivo de la infraestructura de red del distrito.

VII. Sanciones y cancelación de cuentas

A. Los empleados autorizados del distrito serán responsables de determinar qué constituye una violación de estos procedimientos o de la política del Consejo correspondiente. Los empleados autorizados del distrito tienen el derecho de interceptar o leer el correo electrónico de un estudiante, revisar cualquier material, editar o eliminar cualquier material que crean que pueda ser ilegal, obsceno, difamatorio, abusivo o de cualquier otra manera objetable.

B. Si el distrito tiene la intención de imponer cualquier sanción, aparte de revocar los privilegios durante el resto del año escolar, el usuario tendrá derecho al debido proceso legal apropiado.

C. Una cuenta será cancelada cuando:
   1. el padre o tutor del estudiante solicite por escrito al director que la cuenta sea cancelada;
   2. cualquier empleado autorizado del distrito determine que la cuenta debe ser cancelada; o
   3. un estudiante deje el distrito.

VIII. Información privada

Nada es privado en la red. Un estudiante no puede esperar privacidad respecto a sus comunicaciones al usar Internet. A menudo, los sitios de Internet guardan registros que pueden usarse para identificar lo que el usuario a estado viendo o descargando en Internet. El distrito se reserva el derecho de controlar lo que quiera que el usuario haga en la red.

IX. Seguridad

A. La seguridad es una gran prioridad en las redes informáticas.

B. Si se identifica un problema de seguridad, el usuario debe notificarlo inmediatamente al administrador del sistema. Los estudiantes no deben mostrarle el problema a otros usuarios.
   1. Los usuarios no pueden utilizar Internet para discutir o difundir información sobre problemas de seguridad o sobre cómo obtener acceso no autorizado a sitios, servidores, archivos, etc.
   2. No comparta contraseñas con otros usuarios y cambie las contraseñas con frecuencia.
   3. No abandone una estación de trabajo electrónica sin salir de la red.

C. Los estudiantes deben reportar cualquiera de lo siguiente a un maestro o administrador:
   1. si un estudiante recibe u obtiene información a la que no tiene derecho;
   2. si un estudiante sabe de cualquier uso inapropiado de la red por otros; o
   3. si un estudiante cree que el software de filtrado no está filtrando un sitio o sitios que deberían filtrarse bajo este acuerdo.

X. Descargo de responsabilidad

El distrito no da ninguna garantía de ningún tipo, ya sea expresa o implícita, por los servicios que está proporcionando. Los recursos electrónicos se proporcionan sobre la base de "existen, están disponibles". El distrito no será responsable por cualquier daño que el estudiante

pueda sufrir mientras usa sus recursos electrónicos. Estos daños pueden incluir pero no se limitan a: pérdida de datos como resultado de retrasos, falta de entrega o interrupciones del servicio causadas por el sistema o por la negligencia, error u omisión de un individuo. El distrito no promete ni garantiza el mantenimiento ni actualización de su red o la información contenida en ella. El distrito puede suspender o descontinuar estos servicios en cualquier momento. El uso de cualquier información obtenida a través del sistema de información es por cuenta y riesgo del estudiante. El distrito específicamente niega cualquier responsabilidad por la exactitud o adecuación de la información obtenida a través de recursos electrónicos.

XI. Software de filtrado/bloqueo

De acuerdo con la ley estatal y la Ley de Protección de Internet para Niños, el distrito utiliza y configura consistentemente software de filtrado/bloqueo para bloquear el acceso a sitios y materiales que sean inapropiados, ofensivos, obscenos, que contengan pornografía o que sean dañinos para los estudiantes. El distrito utilizará sus mejores esfuerzos para bloquear el acceso a tales sitios y materiales, pero no puede garantizar la efectividad completa de su software de filtrado/bloqueo.