

4-12 Política de Uso Aceptable de la Tecnología Estudiantil

(A) Propósito

La tecnología proporciona interesantes oportunidades para ampliar el aprendizaje de los estudiantes y educadores. Sin embargo, con esta oportunidad viene la responsabilidad de un uso adecuado. La intención de la política aceptable de uso de la tecnología en el distrito escolar del Condado de Okaloosa es: (a) prevenir el acceso a usuarios sobre su red informática, o prevenir la transmisión de material inadecuado a través del internet, correo electrónico u otras formas de comunicación electrónica directa; (b) prevenir el acceso no autorizado y otras actividades ilegales en línea; (c) prevenir que personas no autorizadas en línea divulguen, usen, o difieran información de identificación personal de menores de edad; y (d) cumplir con la Ley de Protección de Internet para Niños [Pub. L. No. 106-554 and 47 USC 254(h)]. Por lo tanto, la Junta Escolar del Condado de Okaloosa ha adoptado la siguiente política estudiantil de uso aceptable de tecnología para guiar a los estudiantes sobre como acceder y utilizar los recursos electrónicos en las escuelas del Condado Escolar de Okaloosa.

(B) Descripción

El servicio de internet será accesible a todas las Escuelas en el condado de Okaloosa a través de la Red del Condado Escolar de Okaloosa y a través de varios otros proveedores de acceso. La red de las escuelas en el Condado de Okaloosa no se ha establecido como un servicio de acceso público o como un foro público. Por lo tanto, el Consejo Escolar tiene el derecho de imponer restricciones razonables sobre el material consultado o publicado a través del sistema. También, se espera que los usuarios sigan las reglas expuestas en el Código de Conducta Estudiantil y la ley sobre el uso del Internet. Nuestro objetivo a la hora de proporcionar acceso de internet a la facultad, personal y estudiantes es promover la calidad educativa en el Condado Escolar de Okaloosa facilitando el intercambio de recursos, la innovación y la comunicación.

Es posible que haya algún material o comunicaciones de particulares que no son adecuados para los niños en edad escolar. La Junta Escolar cree firmemente que la información valiosa y la interacción disponible en esta red global, distancia la posibilidad de que los usuarios puedan obtener material incompatible con las metas educativas del distrito.

El Distrito ve la información recopilada en el Internet de la misma manera que ve materiales de referencia identificados por las escuelas. Expresamente, el Distrito apoya los recursos que realzarán el ambiente de aprendizaje al mismo tiempo que proporcionan orientación y supervisión a profesores y personal administrativo. Mientras es imposible controlar todo el material que una red pública, el Distrito ha tomado precauciones razonables para restringir

el acceso a materiales que se consideran dañinos, y a materiales que no apoyan los objetivos educativos aprobados.

(C) Fines Educativos

Esta política se aplica a todos los dispositivos de tecnología, incluyendo pero no limitado a: computadores (portátiles, equipos de escritorio), BYODs (abreviación que significa: traer sus propios equipos), teléfonos celulares, dispositivos inteligentes, tabletas; sin importar si el equipo es propiedad del estudiante o del distrito.

- (1) El acceso a la tecnología es un privilegio y no un derecho. Todos los estudiantes tendrán acceso a recursos e información global en la Web bajo la supervisión escolar en su aula, centro de computación o laboratorio de tecnología.
- (2) El usuario y sus padres deben firmar la forma MIS 5251 del distrito antes de ser otorgado el acceso a la red OCSD o acceso al internet a través de los recursos electrónicos de la escuela. El acceso a los computadores puede ser retirado de un estudiante en cualquier momento por un miembro del personal de la escuela o por los padres/guardián responsable del estudiante.
- (3) Todas las páginas web que los alumnos han creado como parte de un proyecto de la escolar deben referirse a la escuela, educación y/o actividades informativas y deben tener un maestro patrocinador.
- (4) En el caso de casilleros escolares y otras áreas de almacenamiento de información, equipos de almacenamiento electrónico y/o áreas en general, estarán sujetas a inspección en cualquier momento. Los administradores de las escuelas, ya sea directamente o a través de apoyo, pueden ver archivos y comunicaciones para asegurar la integridad del sistema y asegúrese de que los usuarios están usando el sistema responsablemente. Los usuarios no deben esperar que los archivos almacenados en la plataforma tecnológica del distrito sean privados.
- (5) El distrito no puede garantizar los derechos de privacidad en sus sistemas de computadoras. Los padres/Guardián tienen el derecho en cualquier momento de solicitar ver el contenido de los archivos del computador de su estudiante.
- (6) Se espera que los usuarios individuales de la tecnología sigan las reglas generalmente aceptadas por el protocolo de la red.

(D) Normas de Procedimiento

- (1) El Distrito eliminará toda la información del sistema que el personal de la escuela determine como ilegal, obsceno, pornográfico, abusivo o de cualquier otra manera, en violación de esta política, incluyendo todos los elementos considerados como nocivos. El personal escolar referirá a cualquier persona que viole las disposiciones de esta política a acciones disciplinarias. La cancelación de privilegios del usuario y otras consecuencias estarán a disposición del Director de la escuela o de su designado.

- (2) El vandalismo de un sistema de computadores del Distrito causará la cancelación de privilegios y/o acciones de medida disciplinaria que puede incluir la notificación de aplicación de la ley. El vandalismo incluye, pero no es limitado a la: carga o creación de virus informáticos o software similares, el corte o cambio de software y daño físico a hardware electrónico. Los padres/guardianes podrían hacerse financieramente responsables por los daños resultantes del uso indebido de los estudiantes del sistema informático.
- (3) El acceso consiente, descarga o transmisión de cualquier material perjudicial en la violación de cualquier ley federal, ley del Estado o política del distrito son prohibidos. Esto incluye, pero no es limitado a:
 - (a) Cualquier información que viole o infrinja los derechos de cualquier otra persona
 - (b) Cualquier material motivado por odio, fraude, difamatorio, abusivo, obsceno, profano, sexualmente orientado, amenazador, lenguaje de acoso, intimidación, racialmente ofensivo o material ilegal
 - (c) Cualquier información o comunicación que fomente el uso ilegal de sustancias controladas o promueva el comportamiento criminal
 - (d) Cualquier material que viole las leyes de copyright
- (4) Todos los recursos electrónicos deben ser utilizados de manera responsable, eficiente, ética y legal. Los usuarios deben reconocer su entendimiento sobre esta política como una condición para usar los recursos tecnológicos. Los usos aceptables del Internet son actividades que apoyan el aprendizaje, el trabajo de colaboración y la enseñanza.

(E) Usos Inaceptables

- (1) Cualquier acceso no autorizado a cualquier sistema es ilegal y será tratado como tal. Usos inaceptables del servicio de internet incluyen, pero no se limitan a lo siguiente:
 - (a) La violación de la condición del Código de Conducta Estudiantil, especialmente aquellos que tratan con los derechos de confidencialidad de los estudiantes.
 - (b) Descargar material inapropiado para su uso personal (por ejemplo archivos, gráficos, música y/o películas).
 - (c) Re-publicar comunicaciones personales sin el consentimiento previo del autor.
 - (d) Grabar y volver a transmitir imágenes, vídeos, etc. sin el consentimiento de los sujetos.
 - (e) Copiar comercialmente un software incurriendo en violación de las leyes de derechos de autor u otros materiales protegidos por el copyright, incluyendo fotografías.

- (f) Instalar o almacenar cualquier software en cualquier computador del Distrito sin el permiso del profesor o un empleado responsable del computador.
 - (g) Hacer o intentar hacer cambios en cualquier configuración, contraseña o programa en cualquier sistema informático sin autorización.
 - (h) Usar cualquier computador del Distrito sin permiso del profesor o empleado responsable de ese equipo.
 - (i) Hacer uso de vulgaridades o cualquier otro lenguaje inapropiado, imágenes o gestos en internet en cualquier forma, incluso por escrito, forma gráfica, por mensaje telefónico de voz y en tiempo real.
 - (j) Jugar juegos en línea no autorizados o acceder a los medios de comunicación social sin autorización.
 - (k) Dañar computadoras, sistemas informáticos, software, redes de ordenadores o datos pertenecientes al distrito u otra persona.
 - (l) Cualquier intento de alterar la función de la red o tecnología.
 - (m) Utilizar la identificación de usuario o contraseña de otra persona.
 - (n) Revelar el nombre completo, dirección personal, número de seguro social o el número de teléfono de cualquier estudiante, miembro del personal de la escuela o empleados del distrito.
 - (o) El uso de las computadoras del distrito para acceder a correo electrónico personal. El uso debe limitarse a fines educativos solamente y requiere profesor o autorización administrativa.
 - (p) Monitoreo del tráfico en la red para obtener información personal.
 - (q) Intentar tener acceso a nombres de usuario y contraseñas de otros usuarios por cualquier motivo.
 - (r) Acceso remoto a otras redes, computadores, servidores o cualquier otra tecnología sin el permiso del maestro o administrador.
- (2) Tomar o almacenar imágenes inadecuadas o vídeos. Cualquier violación de esta política también es una violación de las leyes federales o estatales; también puede dar lugar a una acción penal.

(F) Dispositivos Móviles

(1) Normas de Uso Aceptable de Dispositivos Móviles:

- (a) A menos que usted esté expresamente permitido por el instructor para utilizar su dispositivo móvil o aplicaciones en su dispositivo móvil para una tarea de aula, los estudiantes acuerdan no:

(1) Tener sus dispositivos móviles afuera o sobre (se aplicara la política escolar regular)

(2) Text

(3) Hacer llamadas

(4) Jugar juegos de mesa

(5) Activar el Bluetooth

(6) Tomar fotografías o videos

(7) utilizar cualquier otra aplicación no mencionada anteriormente

(b) Los estudiantes comprometen a respetar su dispositivo móvil planes (con los padres). Los estudiantes no tendrán acceso a internet móvil. Durante días en que los dispositivos móviles son usados en la clase, los estudiantes tendrán sus dispositivos móviles en su área de trabajo a la vista. Los estudiantes se comprometen a respetar todas las normas escolares específicas para dispositivos móviles.

(c) Las consecuencias de la violación de las Reglas de Dispositivos Móviles pueden ser, pero no se limitan a lo siguiente:

(1) La primera vez que un estudiante viole las Reglas del Uso Aceptable de Dispositivos Móviles, el estudiante perderá sus privilegios de participación en actividades del aula digital para una 1 semana. Su dispositivo móvil será confiscado por el resto del período de clase por parte del profesor.

(2) La segunda vez que un estudiante viole las Reglas del Uso Aceptable de Dispositivos Móviles, el estudiante perderá sus privilegios de participación en actividades del aula digital para dos 2 semanas. Su dispositivo móvil será confiscado y pasará a disposición de la oficina. Esto puede resultar en una referencia a la oficina.

(3) La tercera vez que un estudiante viole las Reglas del Uso Aceptable de Dispositivos Móviles, el estudiante perderá sus privilegios de usar el dispositivo móvil en la escuela. El dispositivo móvil será confiscado y pasará a disposición a la oficina y resultará en una referencia a la oficina.

(G) Dispositivos Inteligentes y Pruebas

Los dispositivos inteligentes, incluyen pero no se limitan a teléfonos celulares, relojes inteligentes, tabletas, algunas calculadoras. Se puede prohibir el uso de/acceso de estos durante un entorno de pruebas. Los profesores/administradores deberían tener un lugar seguro para almacenar tales dispositivos.

(H) Limitación de Responsabilidad

La Junta Escolar no ofrece garantías de ningún tipo, ya sea expresa o implícita, por el servicio que está proporcionando. El Consejo escolar no será responsable de ningún daño que un usuario pueda sufrir, incluso la pérdida de datos. La junta escolar no será responsable por la exactitud o calidad de la información obtenida a través de cualquier conexión de internet del distrito. Los padres indemnizarán el Distrito contra cualquier daño que sea causado por el uso inadecuado del sistema por parte del estudiante.

(I) Protección Contra Virus

- (1) Los usuarios deben evitar conscientemente o inadvertidamente difundir virus informáticos.
 - (a) No descargar archivos de fuentes desconocidas.
 - (b) Siempre descargue archivos a un computador que tiene una adecuada detección de virus y protección instalada.
 - (c) Las tentativas deliberadas de degradar o interrumpir el rendimiento del sistema serán vistas como actividad criminal en virtud de la legislación estatal y/o de la ley federal.
 - (d) Las escuelas deben escanear todos los medios de almacenamiento de información en busca de virus antes de ser utilizado en computadoras del distrito.
 - (e) No conecte ningún computador o dispositivo electrónico al Internet a menos que haya sido aprobado por el director de proyectos del Distrito, Dustin Keith.

(J) Acceso a Material Inapropiado

En la medida que sea posible, se utilizarán medidas de protección tecnológica (o "filtros de internet") para bloquear o filtrar el servicio de internet, u otras formas de comunicación electrónica, acceso a información inadecuada. Concretamente, tal y como lo exige la Ley de Protección Infantil en Internet (CIPA), el bloqueo será aplicado a representaciones visuales de material considerado como obsceno o de pornografía infantil, o cualquier material considerado perjudicial para menores de edad. Sujeto a supervisión del equipo de personal, las medidas tecnológicas de protección pueden ser desactivadas para adultos o, en el caso de menores de edad, minimizado sólo para investigación auténtica u otros objetivos legales.

(K) Uso Inadecuado de la Red

En la medida en que sea práctico, se tomarán medidas para promover la seguridad y protección de los usuarios de la red de computadoras del distrito, al utilizar el correo electrónico, redes sociales, mensajería instantánea y otras formas de comunicación electrónica directa. Expresamente, como lo requerido por CIPA, la prevención del uso de la red inadecuado incluye: (a) acceso no autorizado, incluidos los identificados como "piratería informática", y otras actividades ilícitas; y (b) divulgación no autorizada, uso y/o divulgación de información de identificación personal de menores.

(L) Educación, Supervisión y Seguimiento

- (1) Debe ser la responsabilidad de todos los miembros del personal del Distrito, incluso, pero no limitado al personal educacional en la escuela para educar, supervisar y vigilar el uso apropiado de la red informática y el acceso al internet en conformidad con la política, la Ley de *“Children’s Internet Protection Act, the Neighborhood Children’s Internet Protection Act, and the Protecting Children in the 21st Century Act”*.
- (2) El Distrito, independientemente o a través de los proveedores tecnológicos contratados, tienen derecho a monitorear de forma remota la red de tráfico y estaciones PC de trabajo con el fin de mantener la seguridad en la red, solucionar problemas de reparación de computadoras, y asistir con problemas relacionados con la tecnología.
- (3) Los procedimientos para desactivar o modificar las medidas tecnológicas de protección será responsabilidad del Superintendente o representantes designados.
- (4) Las escuelas proporcionarán formación adecuada de acuerdo a la edad de los estudiantes que usan sus servicios de internet. La capacitación será diseñada para promover el compromiso del distrito con:
 - (a) Los estándares y uso aceptable de servicios de Internet como sea dispuesto en la política de Uso Aceptable de Tecnología.
 - (b) Seguridad de los estudiantes con respecto a:
 - (1) Seguridad en internet
 - (2) Comportamiento apropiado mientras se está en línea, en sitios web de medios sociales
 - (3) Concienciación y respuesta sobre el ciberacoso
 - (c) Cumplimiento con los requisitos de E-rate de la ley de protección de los niños usando Internet.

Tras recibir esta formación, el estudiante reconocerá que él o ella recibieron el entrenamiento, lo entendió y seguirá las disposiciones de la política del Distrito sobre el uso aceptable de tecnología estudiantil.

Autoridad Legal Estatutaria: Secciones 1001.41(2);1001.42, Estatutos de la Florida

Leyes Puestas en Práctica: Sección 1001.43(3)(A), estatutos de la Florida; 254(h) 47 USC; Ley pública 106-554

Aprobado: Noviembre ____ del 2015