



Título: Política de Uso Aceptable de la Tecnología e Internet para Estudiantes

Código: 04-12

Sección: Capítulo 04 - Estudiantes

04-12 POLÍTICA DE USO ACEPTABLE DE LA TECNOLOGÍA E INTERNET PARA ESTUDIANTES

(A) Propósito

La tecnología ofrece oportunidades emocionantes para ampliar el aprendizaje de los estudiantes y educadores. Sin embargo, con esta oportunidad surge la responsabilidad de utilizarla adecuadamente. El propósito de la Política de Uso Aceptable de la Tecnología e Internet del Distrito Escolar del Condado de Okaloosa es: (a) impedir que los usuarios accedan, a través de su red informática, a material inapropiado o lo transmitan mediante internet, correo electrónico u otras formas de comunicación electrónica directa; (b) impedir el acceso no autorizado y otras actividades ilícitas en línea; (c) impedir la divulgación, el uso o la difusión no autorizados en línea de información de identificación personal de menores; y (d) cumplir con la Ley de Protección de los Niños en Internet [Ley Pública Núm. 106-554 y 47 USC 254(h)]. Por lo tanto, la Junta Escolar del Condado de Okaloosa ha adoptado la siguiente Política de Uso Aceptable de la Tecnología e Internet para Estudiantes a fin de orientar a los estudiantes cuando accedan y utilicen los recursos electrónicos de las Escuelas del Condado de Okaloosa.

(B) Descripción general

El acceso a internet estará disponible para todas las Escuelas del Condado de Okaloosa a través de la Red de las Escuelas del Condado de Okaloosa. La Red de las Escuelas del Condado de Okaloosa no se ha establecido como un servicio de acceso público ni como un foro público. Por lo tanto, la Junta Escolar tiene derecho a imponer restricciones razonables sobre el material al que se acceda o que se publique mediante el sistema. También se espera que los usuarios cumplan las normas establecidas en el Código de Conducta Estudiantil y la ley al utilizar internet. Nuestro objetivo al proporcionar acceso a internet al cuerpo docente, al personal y a los estudiantes es promover la excelencia educativa en las Escuelas del Condado de Okaloosa facilitando el intercambio de recursos, la innovación y la comunicación.

El Distrito considera la información obtenida de internet de la misma manera que los materiales de referencia seleccionados por las escuelas. Específicamente, el Distrito apoya los recursos que mejoren el entorno de aprendizaje, a la vez que el cuerpo docente y el personal escolar brindan orientación y supervisión. Aunque es imposible controlar todo el material de una red pública, el Distrito ha tomado precauciones razonables para restringir el acceso a materiales que considera perjudiciales y a materiales que no respaldan los objetivos educativos aprobados.

(C) Propósitos educativos

Esta política se aplica a todos los dispositivos tecnológicos, incluidos, entre otros: computadoras (portátiles, de escritorio y Chromebook), dispositivos BYOD ("Trae tu propio dispositivo"), teléfonos celulares, dispositivos inteligentes, gafas inteligentes, incluidas las gafas inteligentes graduadas, y tabletas; independientemente de que el dispositivo sea propiedad del estudiante o del Distrito. Esta política también describe el uso y el acceso a internet proporcionado por el Distrito Escolar.

- (1) El acceso a la tecnología es un privilegio y no un derecho. Todos los estudiantes tendrán acceso, bajo supervisión escolar y después del filtrado de contenido del Distrito, a recursos informativos de la World Wide Web a través de su salón de clases, centro de medios o laboratorio de tecnología escolar.
- (2) El usuario y sus padres deben firmar el Formulario MIS 5251 del Distrito antes de que se le conceda acceso

a la red del Distrito o a internet mediante los recursos electrónicos de una escuela. El acceso informático de un estudiante puede ser retirado en cualquier momento por un miembro del personal escolar o por los padres/tutores del estudiante.

- (3) Todas las páginas web de estudiantes creadas como parte de un proyecto escolar deben estar relacionadas con la escuela específica, con actividades educativas y/o con información profesional, y deben contar con el patrocinio de un docente.
- (4) Al igual que los casilleros escolares y otras áreas físicas de almacenamiento, los dispositivos y/o espacios de almacenamiento electrónico están sujetos a inspección en cualquier momento. Los administradores escolares, directamente o mediante personal de apoyo, pueden revisar archivos y comunicaciones para garantizar la integridad del sistema y asegurarse de que los usuarios utilicen el sistema responsablemente. Los usuarios no deben esperar que los archivos almacenados en la tecnología del Distrito sean privados. Todas las transmisiones salientes de información no son seguras y se envían bajo el riesgo del usuario.
- (5) El Distrito no puede garantizar derechos de privacidad en sus sistemas informáticos. Los padres/tutores tienen derecho, en cualquier momento, a solicitar ver el contenido de los archivos informáticos de su estudiante.
- (6) El Distrito protegerá la seguridad de los estudiantes cuando utilicen correo electrónico, salas de chat y otras formas de comunicación electrónica directa. Esto se logra mediante:
 - (a) Limitar las comunicaciones por correo electrónico de los estudiantes únicamente a otras direcciones de correo electrónico del Distrito; y
 - (b) Restringir las salas de chat disponibles a los Sistemas de Gestión del Aprendizaje administrados por el Distrito; y
 - (c) Utilizar el cortafuegos o filtro de internet para bloquear salas de chat, correo electrónico u otras herramientas de comunicación no reguladas.
- (7) Se restringe a los estudiantes el acceso a sitios web, aplicaciones web o programas que les exijan proporcionar información de identificación personal (PII), sin permiso del docente o de la administración escolar y sin confirmar que exista un Acuerdo de Privacidad de Datos Estudiantiles, celebrado a través del Distrito, que proteja dicha PII contra la divulgación, el uso o la difusión no autorizados.

D) Pautas de procedimiento

- (1) El Distrito eliminará del sistema toda información que el personal escolar determine que es ilícita, obscena, pornográfica, abusiva, acosadora o que de otro modo infrinja esta política, incluidos todos los elementos considerados material perjudicial. El personal escolar remitirá para medidas disciplinarias a toda persona que infrinja las disposiciones de esta política. La cancelación de privilegios de usuario y otras consecuencias quedarán a discreción del director de la escuela o su designado.
- (2) El vandalismo de un sistema informático del Distrito dará lugar a la cancelación de privilegios y/o medidas disciplinarias que pueden incluir la notificación a las autoridades del orden público. El vandalismo incluye, entre otras cosas: cargar o crear virus informáticos o programas similares, piratear o alterar programas y causar daños físicos a equipos electrónicos. Los padres/tutores pueden ser considerados económicamente responsables de cualquier daño resultante del uso indebido del sistema informático por parte de su estudiante.
- (3) Se prohíbe acceder, descargar o transmitir intencionalmente cualquier material perjudicial en contravención de cualquier ley federal, ley estatal o política del Distrito. Esto incluye, entre otros:
 - (a) Cualquier información que viole o infrinja los derechos de otra persona

- (b) Cualquier lenguaje o material motivado por el odio, fraudulento, difamatorio, abusivo, obsceno, profano, de naturaleza sexual, amenazante, acosador, intimidatorio, racialmente ofensivo o ilegal
- (c) Cualquier información o comunicación que fomente el uso ilegal de sustancias controladas o promueva conductas delictivas
- (d) Cualquier material que infrinja las leyes de derechos de autor
- (4) Todos los recursos electrónicos deben utilizarse de manera responsable, eficiente, ética y legal. Como condición para utilizar los recursos tecnológicos, los usuarios deben reconocer que comprenden esta política. Los usos aceptables de internet son las actividades que apoyan el aprendizaje, el trabajo colaborativo y la enseñanza.

(E) Usos inaceptables

- (1) Intentar acceder sin autorización a cualquier sistema informático es ilegal y se tratará como tal. Los usos inaceptables de internet incluyen, entre otros, los siguientes:
 - (a) Infringir las disposiciones del Código de Conducta Estudiantil, especialmente las relacionadas con el derecho de los estudiantes a la privacidad.
 - (b) Descargar materiales inapropiados para uso personal (p. ej., archivos, gráficos, música y/o películas).
 - (c) Volver a publicar comunicaciones personales sin el consentimiento previo del autor.
 - (d) Grabar en video y retransmitir imágenes, videos, etc., sin el consentimiento de la persona.
 - (e) Copiar programas comerciales infringiendo las leyes de derechos de autor u otros materiales protegidos por derechos de autor, incluidas fotografías. Tomar o almacenar imágenes o videos inapropiados.
 - (f) Instalar o almacenar cualquier programa en una computadora del Distrito sin el permiso del docente o miembro del personal responsable de la computadora.
 - (g) Realizar o intentar realizar cambios en cualquier configuración, contraseña o programa de un sistema informático sin permiso.
 - (h) Utilizar una computadora del Distrito sin el permiso del docente o miembro del personal responsable de esa computadora.
 - (i) Usar vulgaridades o cualquier otro lenguaje, imagen o gesto inapropiado en internet, de cualquier forma, incluida la escrita, gráfica, telefónica por voz y en tiempo real.
 - (j) Jugar juegos en línea no autorizados.
 - (k) Acceder a datos, información o actividades (incluida la piratería informática) considerados ilícitos.
 - (l) Acceder a plataformas de redes sociales mediante el acceso a internet proporcionado por el Distrito, excepto cuando un docente lo indique expresamente y exclusivamente con fines educativos.
 - (m) Ver o utilizar TikTok, o cualquiera de los servicios de sus plataformas sucesoras, en dispositivos propiedad del Distrito o mediante el acceso a internet proporcionado por el Distrito. TikTok, o cualquier plataforma sucesora, no podrá utilizarse para comunicarse con una escuela, club patrocinado por una escuela, organización extracurricular o equipo deportivo, ni para promocionarlos.
 - (n) Dañar computadoras, sistemas informáticos, programas, redes informáticas o datos pertenecientes al Distrito o a otra persona.

- (o) Intentar interrumpir el funcionamiento de la tecnología o la red.
 - (p) Utilizar los nombres de usuario o contraseñas de otra persona.
 - (q) Revelar el nombre completo, domicilio, número de Seguro Social o número telefónico de cualquier estudiante, miembro del personal escolar o empleado del Distrito.
 - (r) El uso de computadoras del Distrito para acceder al correo electrónico personal debe limitarse únicamente a fines educativos y requiere la aprobación de un docente o administrador.
 - (s) Supervisar el tráfico de la red para obtener información personal.
 - (t) Acceder remotamente a otras redes, computadoras, servidores u otra tecnología sin permiso de un docente o administrador.
 - (u) Intentar obtener acceso a los nombres de usuario y contraseñas de otros usuarios por cualquier motivo.
 - (v) Tomar, grabar o almacenar imágenes o videos no autorizados o inapropiados.
 - (w) Practicar "sexting" en cualquier momento en propiedad escolar o durante funciones escolares. Según la ley de Florida, sexting es la transmisión o distribución consciente a otro menor, por medio de una computadora o dispositivo similar, de cualquier fotografía o video de una persona que muestre desnudez y sea perjudicial para menores. El sexting también incluye poseer una fotografía de cualquier persona, transmitida o distribuida por otro menor, que muestre desnudez. Tal conducta no solo puede ser peligrosa para los estudiantes involucrados, sino que puede ocasionar la exposición no deseada de los mensajes e imágenes a otras personas y podría dar lugar a infracciones penales relacionadas con la transmisión o posesión de pornografía infantil. Tal conducta estará sujeta a medidas disciplinarias y a la posible confiscación de los dispositivos de comunicación inalámbrica.
- (2) Las consecuencias por infringir la Política de Uso Aceptable de la Tecnología para Estudiantes se encuentran en el Código de Conducta Estudiantil. Toda infracción de esta política que también constituya una infracción de una ley federal o estatal puede dar lugar a un proceso penal.

(F) Dispositivos de comunicación inalámbrica

- (1) Reglas de uso aceptable de los dispositivos de comunicación inalámbrica:
 - (a) De conformidad con las disposiciones de la ley de Florida, un estudiante puede poseer dispositivos de comunicación inalámbrica mientras se encuentre en propiedad escolar o asista a una función escolar. Salvo que esta política disponga lo contrario, dichos dispositivos deben estar apagados y guardados de forma segura y en silencio durante la jornada escolar. A efectos de esta política, los dispositivos de comunicación inalámbrica o dispositivos móviles incluyen teléfonos celulares, tabletas electrónicas, lectores electrónicos, gafas inteligentes, incluidas las gafas inteligentes graduadas, u otros dispositivos similares de comunicación inalámbrica; sin embargo, a efectos de esta política, un estudiante no puede poseer gafas inteligentes, incluidas las gafas inteligentes graduadas, en propiedad de la Junta Escolar, en el transporte del distrito escolar ni mientras asiste a una función escolar, salvo autorización expresa conforme a la sección 1006.07(2)(f)(2) de los Estatutos de Florida.
 - (b) Los estudiantes de escuela primaria y secundaria intermedia no pueden utilizar un dispositivo personal de comunicación inalámbrica durante la jornada escolar, salvo que sea necesario para supervisar una afección médica, facilitar una adaptación por discapacidad o utilizarlo en un lugar designado dentro del edificio escolar expresamente autorizado por el director. Se deberá proporcionar la documentación correspondiente a la escuela antes de que el director autorice dicho uso.
 - (c) Los dispositivos de alerta médica deben registrarse en la clínica de salud escolar. Para estudiantes

con discapacidades, los dispositivos de asistencia deben estar aprobados en el IEP, Plan 504 o plan individual de salud escolar del estudiante. El uso indebido de estos dispositivos puede dar lugar a medidas disciplinarias.

- (d) Salvo que lo permita el docente de escuela secundaria, un administrador escolar o esté autorizado en el IEP o Plan 504 del estudiante, durante la jornada escolar, incluso fuera del plantel en una excursión y en eventos patrocinados por la escuela, los estudiantes no deberán:
 - (i) Tener sus dispositivos móviles a la vista (se aplica la política regular de la escuela/del Distrito)
 - (ii) Enviar mensajes de texto
 - (iii) Hacer llamadas
 - (iv) Jugar
 - (v) Activar Bluetooth
 - (vi) Tomar fotografías o videos
 - (vii) Utilizar cualquier otra aplicación no mencionada anteriormente
- (e) Los estudiantes de escuela secundaria superior que utilicen sus dispositivos móviles personales en el salón de clases deberán acceder a las funciones en línea únicamente a través de la red del Distrito. Se prohíbe a todos los estudiantes utilizar cualquier dispositivo de grabación, incluidos, entre otros, dispositivos de comunicación inalámbrica, cámaras, grabadoras de audio u otros equipos electrónicos o mecánicos, para captar, grabar o transmitir palabras (es decir, audio) y/o imágenes (es decir, fotografías o video) de cualquier estudiante, miembro del personal u otra persona en la escuela o mientras asisten a una actividad relacionada con la escuela durante la jornada escolar, sin notificación previa expresa a dichas personas y sin el consentimiento explícito del director o su designado para captar, grabar o transmitir tales palabras o imágenes. El uso de un dispositivo de comunicación inalámbrica o cualquier otro dispositivo electrónico, mecánico o de grabación para tomar o transmitir audio y/o fotografías/videos de una persona sin su consentimiento se considera una invasión de la privacidad y no está permitido.
- (f) Los dispositivos de comunicación inalámbrica, incluidos, entre otros, aquellos con cámaras, no podrán activarse ni utilizarse en ningún momento en situaciones escolares donde exista una expectativa razonable de privacidad personal. Estos lugares y circunstancias incluyen, entre otros, vestuarios, instalaciones de duchas, baños y cualquier otra área donde los estudiantes u otras personas puedan cambiarse de ropa o estar en cualquier etapa o grado de desnudez o cambio de ropa. El Superintendente y los directores están autorizados para determinar otros lugares y situaciones específicos donde el uso de un dispositivo esté absolutamente prohibido.
- (g) Los estudiantes no tendrán expectativa alguna de confidencialidad respecto del uso de sus dispositivos de comunicación inalámbrica en propiedad escolar o en eventos patrocinados por el Distrito.
- (h) Se prohíbe a los estudiantes utilizar dispositivos de comunicación inalámbrica de cualquier manera que razonablemente pudiera generar en otra persona la impresión de estar amenazada, humillada, acosada, avergonzada o intimidada.
- (i) Se prohíbe a los estudiantes utilizar dispositivos de comunicación inalámbrica para captar y/o transmitir información de exámenes o cualquier otra información de una manera que constituya fraude, robo, trampa o deshonestidad académica. Asimismo, se prohíbe a los estudiantes utilizar dispositivos de comunicación inalámbrica para recibir dicha información.
- (j) Los docentes de escuela secundaria superior designarán un área del salón de clases para el almacenamiento seguro de los dispositivos de comunicación inalámbrica durante el tiempo de instrucción.
- (k) Sin perjuicio de cualquier disposición contraria de esta política, mientras se encuentren en el transporte del Distrito, y sujetos a las disposiciones de uso aceptable de esta política, los estudiantes podrán utilizar sus dispositivos móviles personales para actividades que no causen interrupciones, como completar trabajos escolares, leer, escuchar música en privado con audífonos, enviar mensajes de texto o jugar. Se prohíbe a los estudiantes utilizar dispositivos de comunicación inalámbrica para captar, grabar o transmitir palabras (es decir, audio) y/o imágenes (es decir, fotografías o video) de cualquier estudiante, miembro del personal u otra persona mientras se

encuentren en el transporte del Distrito, sin notificación previa expresa a dichas personas y sin el consentimiento explícito del conductor del autobús para captar, grabar o transmitir tales palabras o imágenes. El uso de un dispositivo de comunicación inalámbrica para tomar o transmitir audio y/o fotografías/videos de una persona sin su consentimiento se considera una invasión de la privacidad y no está permitido. El uso adecuado de los dispositivos móviles personales está bajo la dirección del conductor y/o asistente del autobús. El incumplimiento de las instrucciones dadas por el conductor y/o asistente del autobús puede dar lugar a las consecuencias disciplinarias establecidas en esta política.

- (I) Las consecuencias por infringir esta política sobre Dispositivos de Comunicación Inalámbrica se encuentran en el Código de Conducta Estudiantil. Toda infracción de esta política que también constituya una infracción de leyes federales o estatales puede dar lugar a un proceso penal.

(G) Dispositivos inteligentes y exámenes

Puede prohibirse el uso o porte de dispositivos inteligentes, incluidos, entre otros, teléfonos celulares, relojes inteligentes, tabletas y algunas calculadoras, durante un entorno de exámenes. Los docentes/administradores deben disponer de un lugar seguro para guardar dichos dispositivos.

(H) Limitación de responsabilidad

La Junta Escolar no ofrece garantías de ningún tipo, expresas o implícitas, respecto del servicio que proporciona. La Junta Escolar no será responsable de ningún daño que pueda sufrir un usuario, incluida la pérdida de datos. La Junta Escolar no será responsable de la exactitud ni de la calidad de la información obtenida mediante cualquier conexión a internet del Distrito. Los padres indemnizarán al Distrito por cualquier daño causado por el uso inapropiado del sistema por parte del estudiante.

(I) Protección contra virus informáticos

- (1) Los usuarios deben evitar propagar virus informáticos, ya sea consciente o inadvertidamente.

- (a) No descargue archivos de fuentes desconocidas.
- (b) Descargue siempre los archivos en una computadora que tenga instalada una protección y detección de virus adecuada.
- (c) Los intentos deliberados de degradar o interrumpir el funcionamiento del sistema se considerarán actividad delictiva conforme a las leyes estatales y/o federales aplicables.
- (d) Las escuelas deben analizar todos los medios de almacenamiento para detectar virus antes de utilizarlos en computadoras del Distrito.
- (e) No conecte ninguna computadora ni dispositivo electrónico a internet, salvo que haya sido aprobado por el Especialista en Gestión de Puestos del Distrito.

(J) Acceso a material inapropiado

En la medida de lo posible, se utilizarán medidas de protección tecnológica (o “filtros de internet”) para bloquear o filtrar el acceso, mediante internet u otras formas de comunicación electrónica, a información inapropiada. Específicamente, según lo exige la Ley de Protección de los Niños en Internet (CIPA), el bloqueo se aplicará a representaciones visuales de material considerado obsceno o pornografía infantil, o a cualquier material considerado perjudicial para menores. Bajo supervisión del personal, las medidas de protección tecnológica podrán desactivarse para adultos o, en el caso de menores, reducirse únicamente para investigaciones legítimas u otros fines lícitos.

(K) Uso inapropiado de la red

En la medida de lo posible, se tomarán medidas para promover la seguridad de los usuarios de la red informática en línea del Distrito cuando utilicen correo electrónico, redes sociales, mensajería instantánea y otras formas de comunicación electrónica directa.

Específicamente, según lo exige la CIPA, la prevención del uso inapropiado de la red incluye: (a) el acceso no autorizado, incluida la denominada “piratería informática”, y otras actividades ilícitas; y (b) la divulgación, el uso y/o la difusión no autorizados de información de identificación personal de menores.

(L) Educación, supervisión y monitoreo

- (1) Será responsabilidad de todos los miembros del personal del Distrito, incluido, entre otros, el personal docente

de cada plantel, educar, supervisar y monitorear el uso apropiado de la red informática en línea y el acceso a internet de conformidad con esta política, la Ley de Protección de los Niños en Internet, la Ley de Protección de los Niños del Vecindario en Internet y la Ley de Protección de los Niños en el Siglo XXI.

- (2) El Distrito, de forma independiente o mediante proveedores de tecnología contratados, tiene derecho a monitorear remotamente el tráfico de la red y las estaciones de trabajo informáticas con el fin de mantener la seguridad de la red, solucionar reparaciones de computadoras y ayudar con problemas relacionados con la tecnología.
- (3) Los procedimientos para desactivar o modificar de cualquier otro modo las medidas de protección tecnológica serán responsabilidad del Superintendente o su designado.
- (4) Las escuelas proporcionarán capacitación apropiada para la edad a los estudiantes que utilicen sus instalaciones de internet. La capacitación estará diseñada para promover el compromiso del Distrito con:
 - (a) Las normas y el uso aceptable de los servicios de internet establecidos en esta Política de Uso Aceptable de la Tecnología e Internet para Estudiantes.
- (b) La seguridad de los estudiantes con respecto a:
 - (i) La seguridad en internet
 - (ii) El comportamiento apropiado en línea
 - (iii) Para estudiantes de 6.º a 12.º grado, los efectos sociales, emocionales y físicos de las redes sociales
 - (iv) La concientización y respuesta ante el ciberacoso
- (c) El cumplimiento de los requisitos de E-rate de la Ley de Protección de los Niños en Internet.

Al firmar el Formulario MIS 5251, Política de Uso Aceptable de la Tecnología e Internet para Estudiantes, el estudiante y su padre/madre/tutor reconocerán que recibieron, revisaron y

comprendieron la Política de Uso Aceptable de la Tecnología e Internet para Estudiantes del Distrito, y que cumplirán todas sus disposiciones. Esta política debe firmarse al momento de la matrícula y nuevamente cada año.

Adoptada: 23 de octubre de 2000

Última revisión: 26 de mayo de 2026

Último examen: 14 de octubre de 2024

Fechas de revisiones anteriores: 13 de noviembre de 2007; 9 de noviembre de 2016; 31 de julio de 2018; 24 de julio de 2023;

28 de julio de 2025

Recursos adicionales

Autoridad legal: §§1001.41(2) y 1001.42(28), Estatutos de Florida

Leyes implementadas: §§934.03, 1001.43(3)(A), 1003.02(1), 1003.32(1), 1003.42(2) y 1006.07, Estatutos de Florida; 47 USC 254(h); Ley Pública Núm. 106-554
