



Distrito Escolar Unificado de Bellflower

Acuerdo de Uso Aceptable de la Red, Recursos Digitales e Internet

General

El acceso a internet y a la red, los dispositivos proporcionados por el distrito, el software, las cuentas en línea y el correo electrónico, provistos por el Distrito Escolar Unificado de Bellflower, están destinados para uso educativo, instrucción, investigación y la facilitación de la comunicación, la colaboración y otros fines relacionados con la educación. Esto incluye el acceso y uso de herramientas aprobadas de Inteligencia Artificial (IA), plataformas de redes sociales con fines educativos y otras tecnologías emergentes. Se espera que los usuarios mantengan estándares de cortesía, profesionalismo, ética y respeto al utilizar estas herramientas y recursos proporcionados por el Distrito. Todo uso de los recursos tecnológicos del Distrito debe cumplir con este acuerdo, la Política de Trae Tu Propio Dispositivo (BYOD) de Bellflower USD, la Política de la Mesa Directiva y las leyes aplicables.

Usos prohibidos de la red, los recursos digitales, internet y el correo electrónico

Los usuarios no pueden participar en ninguna de las actividades enumeradas a continuación como prohibidas. Si los usuarios no están seguros de si un comportamiento o uso específico está permitido, deben comunicarse con su maestro o con el director de la escuela antes de realizar la actividad.

Usos prohibidos

- Transmisión o acceso a cualquier material que viole cualquier ley federal o estatal.
- Distribución de información que viole o infrinja los derechos de cualquier otra persona.
- Transmisión o acceso a información que sea difamatoria, inapropiada, abusiva, obscena, profana, de orientación sexual, amenazante, racialmente ofensiva, discriminatoria (basada en cualquier característica protegida), acosadora, intimidatoria, de ciberacoso o ilegal.
- Anuncios, solicitudes, empresas comerciales o cabildeo político que no hayan sido aprobados previamente por la administración del Distrito.
- Transmisión o acceso a información que fomente el uso de sustancias controladas o el uso del sistema con el propósito de incitar al crimen o a la violencia.
- Material que viole la ley de propiedad intelectual, incluido el intercambio no autorizado de música, videos, software o cualquier otro material bajo derechos de autor. Esto incluye el plagio, como

presentar como propio el trabajo generado por cualquier herramienta de IA sin la debida atribución o permiso, y el uso o la reproducción no autorizados de contenido generado por herramientas de IA cuando el usuario no posea los derechos para hacerlo.

- Dañar los equipos informáticos o de red, dispositivos, archivos, datos o el sistema de internet de cualquier manera (incluida la difusión deliberada o negligente de virus informáticos, el vandalismo de datos, la alteración no autorizada de las configuraciones de hardware o software del Distrito, o la participación en conductas que puedan interferir o interrumpir el entorno educativo o empresarial del Distrito). Los estudiantes que utilicen dispositivos personales en la red del Distrito deben asegurarse de que sus dispositivos mantengan una protección antivirus y contra malware actualizada.
- Obtener o intentar obtener acceso no autorizado a los sistemas de red e internet del Distrito, a las cuentas o archivos de otros usuarios, o a cualquier sistema de terceros por cualquier medio (por ejemplo, *phishing*, *hacking*, alteración maliciosa, compartir o revelar contraseñas a cualquier persona que no sean sus propios padres o tutores, etc.). Los usuarios son responsables de la seguridad de sus contraseñas y cuentas.
- Intentar obtener acceso a material que está bloqueado o filtrado por el Distrito. Está prohibido cualquier intento de eludir los filtros de red del Distrito.
- Utilizar los recursos tecnológicos del Distrito, incluido el ancho de banda de la red WiFi del Distrito con dispositivos personales, para un uso personal no educativo que sea excesivo o interfiera con las actividades educativas.
- Utilizar cuentas proporcionadas por el Distrito (por ejemplo, correo electrónico, plataformas de aprendizaje) para cualquier actividad personal o no relacionada con el distrito, incluidas las redes sociales personales.
- Crear, acceder o transmitir una representación visual identificable de sí mismo o de otro estudiante menor de 18 años (pornografía infantil).
- Falsificar la identidad propia o asumir la identidad de otra persona (suplantación de identidad falsa), lo que incluye enviar correos electrónicos anónimos o crear perfiles falsos con fines maliciosos.
- Hacer trampa o deshonestidad académica, lo que incluye el uso de tecnología o herramientas de IA para completar tareas o exámenes de una manera no autorizada por el maestro.
- Utilizar "plataformas de IA no supervisadas" sin el permiso explícito y la guía del maestro.
- Grabar la voz o la imagen de otra persona sin su consentimiento, o de cualquier manera que interrumpa el entorno educativo o invada la privacidad.

El Distrito se reserva el derecho de tomar medidas inmediatas si ocurre cualquiera de los siguientes casos:

- La actividad o el comportamiento del estudiante en la red o con los recursos digitales del Distrito crea un problema de seguridad para el personal, los estudiantes, la red o los recursos de internet.
- El uso que el estudiante haga de los recursos del Distrito sea de formas que el Distrito determine que carecen de usos legítimos y aprobados, o que se consideren inapropiadas.

Filtrado y monitoreo

Si bien es imposible controlar todo el contenido en internet, el Distrito cuenta con un filtro de red. En cumplimiento con la Ley de Protección de Internet para Niños (CIPA), el Distrito bloquea o filtra el contenido en la red/internet del Distrito que se considere inapropiado para menores, que carezca de contenido educativo o

relacionado con el trabajo, o que represente una amenaza para la red. Los usuarios no deberán utilizar ningún sitio web, aplicación ni ningún otro método para eludir el filtrado de la red ni realizar otras actividades ilegales. El Distrito monitorea el uso de su red y recursos digitales para garantizar el cumplimiento de este acuerdo y las leyes aplicables. Los usuarios no deben tener expectativas de privacidad en el uso que hagan de los recursos tecnológicos del Distrito, incluidos el correo electrónico, el acceso a internet y los archivos almacenados en los sistemas del Distrito, excepto según lo dispuesto por la ley. Los dispositivos personales utilizados en la red escolar están sujetos a inspección por parte de los administradores escolares si se sospecha una violación de la política de la escuela o del distrito.

Manejo de datos

De conformidad con la Ley de Protección de la Privacidad de los Niños en Línea (COPPA), el distrito se compromete a proteger la privacidad y la seguridad de los datos de los estudiantes al utilizar sitios web, aplicaciones y servicios en línea educativos. Cada año, el distrito solicitará un permiso que le permita actuar como agente de los padres para otorgar el consentimiento para la recopilación y el uso de la información del estudiante dentro del contexto escolar.

Este enfoque está permitido bajo la Regla COPPA de la FTC cuando la información del estudiante se utiliza exclusivamente con fines educativos y no para fines comerciales u otros usos no relacionados. Al aceptar este acuerdo, usted, como padre, madre o tutor legal, reconoce y acepta que el distrito actúe como su agente bajo COPPA con el propósito de otorgar el consentimiento en su nombre para la recopilación y el uso de la información personal de su hijo por parte de sitios web, aplicaciones y servicios en línea educativos utilizados dentro del entorno escolar.

Al otorgar este permiso, los padres autorizan a la escuela a administrar el acceso a los sitios web y aplicaciones educativas en nombre de su hijo, asegurando que todos los datos recopilados se utilicen únicamente para respaldar el aprendizaje, la instrucción y el progreso académico. El distrito mantiene el control sobre el uso de los datos de los estudiantes y exige que todos los proveedores aprobados se adhieran a limitaciones estrictas sobre el uso de datos. El distrito revisa minuciosamente todos los recursos en línea para garantizar que cumplan con estrictos estándares de privacidad y seguridad de datos. Cualquier información personal recopilada a través de estos servicios se utilizará únicamente de manera consistente con las metas educativas y no se compartirá para marketing, publicidad ni ningún otro propósito comercial no educativo.

Seguridad digital e internet de los estudiantes

Responsabilidades del estudiante

- Los estudiantes no enviarán mensajes abusivos a nadie, ni transmitirán material a nadie que sea amenazante, obsceno, perturbador, sexualmente explícito, protegido por secreto comercial o que pueda interpretarse como acoso o menosprecio hacia otros en función de su raza/etnia, origen nacional, género, orientación sexual, edad, discapacidad, religión o creencias políticas. Esto incluye cualquier forma de ciberacoso o acoso.

- Los estudiantes no deben revelar información personal (dirección de casa, número de teléfono, fecha completa de nacimiento, contraseñas u otros datos confidenciales) sobre sí mismos o sobre otras personas en sitios de redes sociales de acceso público, en salas de chat, en correos electrónicos u otras comunicaciones electrónicas directas, o en cualquier otro foro en internet, a menos que esté específicamente autorizado y guiado por un maestro para un fin educativo.
- Los estudiantes no deben mostrar fotografías o videos de sí mismos o las imágenes de otros sin el consentimiento apropiado y con fines educativos según lo indicado por el personal escolar. Está prohibido grabar a otros sin su consentimiento.
- Los estudiantes no deben conocer en persona a nadie que hayan conocido únicamente a través de internet sin el conocimiento y la aprobación de sus padres o tutores, e idealmente, en un lugar público y seguro con la supervisión de un adulto si los padres o tutores consideran necesaria dicha reunión.
- Los estudiantes deben revelar de inmediato a su maestro u otro empleado de la escuela cualquier mensaje, imagen, video u otra actividad que reciban u observen que sea inapropiada, los haga sentir incómodos o que consideren que viola este acuerdo.
- Los estudiantes no deben permitir que ningún dispositivo (proporcionado por el Distrito o dispositivos personales utilizados para fines escolares) guarde sus contraseñas, y deben cerrar la sesión de sus cuentas cuando terminen de usar un dispositivo compartido o público.
- Los estudiantes respetarán los derechos de autor, incluida la citación adecuada de las fuentes y el cumplimiento de las pautas de uso legítimo (*fair use*). Esto incluye reconocer el uso de herramientas de IA permitidas al generar contenido según las pautas del maestro o del distrito para evitar el plagio.
- Los estudiantes no utilizarán la red ni los recursos digitales del Distrito de ninguna manera que interrumpa el uso de la red por parte de otros.
- Los estudiantes utilizarán las herramientas de IA aprobadas de manera responsable y ética, para el aprendizaje y la investigación según lo permitan sus maestros. No utilizarán la IA para hacer trampa, plagiar, incurrir en una suplantación de identidad falsa o tergiversar su propio trabajo. Serán conscientes de los posibles sesgos e inexactitudes en el contenido generado por IA y evaluarán críticamente dicha información.
- Los estudiantes que utilicen las redes sociales para fines educativos aprobados (por ejemplo, grupos de clase, clubes escolares) mantendrán un tono respetuoso y apropiado, adhiriéndose a todas las demás disposiciones de este AUP. El acceso a las redes sociales personales utilizando las redes o cuentas del Distrito está sujeto a las prohibiciones sobre el uso personal detalladas en este acuerdo y en la política BYOD.
- Los estudiantes son responsables de tomar precauciones para proteger sus datos personales y los datos de los demás al utilizar la tecnología.
- Los estudiantes que participen en el programa BYOD (grados 6 a 12) deben cumplir con la Política BYOD de Bellflower USD, lo que incluye usar los dispositivos con la aprobación del maestro para fines educativos y asegurarse de que su dispositivo esté cargado antes de llegar a la escuela.

Responsabilidades de los padres

- Los padres son los principales responsables de transmitir su conjunto particular de valores familiares a sus hijos.

- Los padres hablarán con sus hijos sobre qué material es aceptable y cuál no lo es para que accedan y creen a través de la tecnología del Distrito y personal, incluidas las redes sociales y las herramientas de IA.
- Los padres son exclusivamente responsables de monitorear el uso que sus hijos hacen de internet y de todos los recursos digitales, incluidas las plataformas de software del Distrito y los dispositivos personales, cuando se acceda a ellos desde el hogar o desde un lugar fuera de la escuela.
- Los padres informarán al maestro de su hijo o a otro empleado de la escuela sobre cualquier mensaje u otra actividad de la que su hijo les informe que sea inapropiada o preocupante mientras utiliza internet u otros recursos digitales para fines escolares.
- Se alienta a los padres a hablar con sus hijos regularmente sobre la seguridad en línea, la ciudadanía digital, el uso responsable de la IA, las preocupaciones sobre el plagio y la suplantación de identidad falsa, así como el contenido de este AUP y la Política BYOD.
- Los padres entienden que, si bien los estudiantes de los grados 6 a 12 pueden traer dispositivos personales a la escuela bajo la política BYOD, el Distrito no es responsable por dispositivos personales perdidos, prestados, dañados o robados.

Violaciones al Acuerdo de Uso Aceptable y a la Política BYOD

El Distrito se reserva el derecho de terminar o restringir el acceso de cualquier usuario a la red, los recursos digitales y los sistemas de internet del Distrito.

Si un estudiante viola este acuerdo o la Política BYOD, se tomarán las medidas disciplinarias apropiadas de acuerdo con la violación, el Código de Educación de California, la Política de la Mesa Directiva, el manual del estudiante y los códigos de las autoridades policiales locales. Los dispositivos utilizados para fines ilegales o en violación de la política pueden ser confiscados. Si se revoca el acceso de un estudiante, este no podrá ser penalizado académicamente. El Distrito se asegurará de que el estudiante continúe teniendo una oportunidad significativa de participar en todos los programas educativos brindados. Las consecuencias pueden incluir, entre otras, la pérdida de los privilegios de acceso, medidas disciplinarias según lo detallado en el código de conducta estudiantil, la confiscación de dispositivos, la restitución por daños y la remisión a las autoridades policiales si corresponde.

Limitación de responsabilidad

El Distrito Escolar Unificado de Bellflower no ofrece garantías de ningún tipo, ya sean expresas o implícitas, por el servicio que brinda. El Distrito Escolar Unificado de Bellflower no es responsable de ninguna reclamación, pérdida, daño, costo u otras obligaciones que surjan del uso de la red o de las cuentas. Esto incluye, pero no se limita a, la pérdida de datos o ingresos que resulten de retrasos, falta de entregas, entregas erróneas o interrupciones del servicio causadas por la propia negligencia del Distrito o por errores u omisiones del usuario. El uso de internet, la red o cualquier recurso digital del Distrito (incluida la red WiFi del Distrito con dispositivos personales) es bajo el propio riesgo del usuario. El Distrito no es responsable de los dispositivos personales en caso de pérdida, préstamo, daño o robo. El Distrito no es responsable de ningún cargo o tarifa no autorizados, incluidos los cargos por datos en cuentas personales en los que se pueda incurrir durante el uso aprobado relacionado con la escuela con dispositivos personales, que resulten del acceso a internet o a

los servicios en línea. El Distrito no es responsable de la precisión ni de la calidad de la información obtenida a través del sistema o almacenada en este.