



Acceptable Use Policy

Corinth School District

El propósito de esta política es proporcionar pautas y reglamentos claros sobre el uso seguro, legal, considerado y responsable de esta tecnología, así como de todos los recursos tecnológicos utilizados por los estudiantes, el personal, los padres y los voluntarios del Distrito Escolar de Corinth. Todos los recursos tecnológicos del Distrito Escolar de Corinth y la información almacenada en ellos se rigen por las políticas del distrito y están sujetos a la supervisión e inspección de la escuela. Esta política se aplica independientemente de si dicho uso se produce dentro o fuera de la propiedad del distrito escolar, y se aplica a todos los recursos tecnológicos del distrito escolar, incluidos, entre otros, las redes y conexiones informáticas, los recursos, las herramientas y los entornos de aprendizaje disponibles por o en las redes, y todos los dispositivos que se conectan a esas redes.

El Distrito Escolar de Corinth se reserva el derecho de monitorear, acceder, recuperar, leer y divulgar todos los mensajes, información y archivos que han sido creados, enviados, publicados, almacenados o utilizados por sus recursos tecnológicos a los funcionarios encargados de hacer cumplir la ley y otros sin noticia anterior. Cualquier individuo que viole esta política o cualquier ley local, estatal o federal aplicable está sujeto a medidas disciplinarias, pérdida de privilegios tecnológicos y puede enfrentar acciones legales.

A. EXPECTATIVAS PARA EL USO DE LOS RECURSOS TECNOLÓGICOS DE LA ESCUELA

Los estudiantes, el personal, solo pueden usar los recursos tecnológicos del distrito escolar y otros expresamente autorizados por el distrito escolar. El uso de los recursos tecnológicos del distrito escolar, incluido el acceso a Internet, es un privilegio, no un derecho. Los usuarios individuales de los recursos tecnológicos del distrito escolar son responsables de su comportamiento y comunicación cuando usan esos recursos. El uso responsable de los recursos tecnológicos del distrito escolar es un uso ético, legal, respetuoso, académicamente honesto y que apoya el aprendizaje de los estudiantes. Cada usuario tiene la responsabilidad de respetar a los demás en la comunidad escolar y en Internet. Se espera que los usuarios cumplan con las reglas generalmente aceptadas de la etiqueta de la red. Los estándares generales de comportamiento de los estudiantes y empleados, incluidos los prescritos en las políticas de la junta aplicables, el Manual para estudiantes y empleados y otras reglamentaciones y reglas escolares, se aplican al uso de Internet y otros recursos tecnológicos escolares.

Además, cualquier persona que use computadoras o dispositivos electrónicos del distrito escolar o que acceda a la red escolar o a Internet usando los recursos del distrito escolar debe cumplir con las reglas adicionales para el uso responsable enumeradas en la Sección B, a continuación. Estas reglas están destinadas a aclarar las expectativas de conducta, pero no deben interpretarse como inclusivas.

Todos los estudiantes y empleados deben ser informados anualmente de los requisitos de esta política y los métodos por los cuales pueden obtener una copia de esta política. Antes de usar los recursos tecnológicos del distrito escolar, los estudiantes y empleados deben firmar una declaración que indique que entienden y cumplirán estrictamente con estos requisitos. El incumplimiento de estos requisitos dará lugar a medidas disciplinarias, incluida la revocación de los privilegios de usuario. El uso indebido deliberado puede dar lugar a medidas disciplinarias y/o acciones penales en virtud de las leyes estatales y federales aplicables.

B. REGLAS PARA EL USO DE LOS RECURSOS TECNOLÓGICOS DE LA ESCUELA

1. Los recursos tecnológicos del distrito escolar se proporcionan para fines relacionados con la escuela solo durante el horario escolar. Los usos aceptables de dichos recursos tecnológicos se limitan a actividades responsables, eficientes y legales que apoyen el aprendizaje y la enseñanza. Se prohíbe el uso de los recursos tecnológicos del distrito escolar con fines políticos o para fines comerciales o lucrativos.
2. Los recursos tecnológicos del distrito escolar son instalados y mantenidos por miembros del Departamento de Tecnología. Los estudiantes y empleados no intentarán realizar ninguna instalación o mantenimiento sin el permiso del Departamento de Tecnología.
3. Bajo ninguna circunstancia se puede copiar el software comprado por el distrito escolar para uso personal.
4. Los estudiantes y empleados deben cumplir con todas las leyes aplicables, incluidas las relacionadas con derechos de autor y marcas comerciales, información confidencial y registros públicos. Cualquier uso que viole las leyes estatales o federales está estrictamente prohibido. El plagio de los recursos de Internet se tratará de la misma manera que hacer trampa, como se indica en el Manual del estudiante.
5. Ningún usuario de recursos tecnológicos, incluidas las personas que envían o reciben comunicaciones electrónicas, puede participar en la creación, la visualización, el acceso, la descarga, el almacenamiento, la impresión o la transmisión intencional de imágenes, gráficos (incluidas imágenes fijas o en movimiento), archivos de sonido, archivos de texto, documentos, mensajes u otro material que sea obsceno, difamatorio, profano, pornográfico, acosador, abusivo o que se considere dañino para menores. Todos los usuarios deben cumplir con todo el manual del estudiante y las políticas del distrito con respecto a la intimidación, el acoso, las amenazas, la violencia y la agresión de los estudiantes, cuando utilicen la tecnología del distrito escolar.
6. Está prohibido el uso de proxies anónimos para eludir el filtrado de contenidos.
7. Los usuarios no pueden instalar ni utilizar ningún programa de intercambio de archivos basado en Internet diseñado para facilitar el intercambio de material protegido por derechos de autor.
8. Los usuarios de los recursos tecnológicos no podrán enviar comunicaciones electrónicas de forma fraudulenta (es decir, falseando la identidad del remitente).
9. Los usuarios deben respetar la privacidad de los demás. Al usar el correo electrónico, salas de chat, blogs u otras formas de comunicación electrónica, los estudiantes no deben revelar información de identificación personal, o información que sea privada o confidencial, como la dirección de la casa o el número de teléfono, información de la cuenta corriente o de crédito o seguridad social, número de ellos mismos o compañeros de estudios. Además, los empleados de la escuela no deben divulgar en los sitios web o páginas web del distrito escolar ni en ningún otro lugar de Internet ninguna información confidencial, privada o de identificación personal sobre los estudiantes (incluidos nombres, direcciones o fotografías) sin el permiso por escrito de un padre o tutor o un representante elegible. estudiante, excepto que lo permita la Ley de Privacidad y Derechos Educativos de la Familia (FERPA). Los usuarios tampoco pueden reenviar o publicar comunicaciones personales sin el consentimiento previo del autor.
10. Los usuarios no pueden dañar intencionalmente o por negligencia las computadoras, los sistemas informáticos, los dispositivos digitales o electrónicos, el software, las redes informáticas o los datos de ningún usuario conectado a los recursos tecnológicos del distrito escolar. Los usuarios no pueden transmitir virus informáticos o mensajes autorreplicantes a sabiendas o por negligencia, ni intentar deliberadamente degradar o interrumpir el rendimiento del sistema. Los usuarios deben escanear cualquier archivo descargado en busca de virus.
11. Los usuarios no pueden crear ni introducir juegos, programas de comunicación en red ni ningún programa o software extranjero en ninguna computadora, dispositivo electrónico o red del distrito escolar sin el permiso expreso del director de tecnología o su designado.

12. Los usuarios tienen prohibido participar en actividades no autorizadas o ilegales, como "piratear" o usar la red informática para obtener o intentar obtener acceso no autorizado o ilegal a otras computadoras, sistemas informáticos o cuentas.
13. Los usuarios tienen prohibido usar la identificación o contraseña de otra persona para cualquier recurso tecnológico sin el permiso de la persona. Los estudiantes también deben tener el permiso del maestro u otro funcionario escolar.
14. El usuario no podrá leer, alterar, cambiar, bloquear, ejecutar o suprimir archivos o comunicaciones pertenecientes a otro usuario sin la previa autorización expresa del titular.
15. Los empleados no deben usar contraseñas o identificaciones de usuario para ningún sistema de datos para un propósito no autorizado o inapropiado.
16. Si un usuario identifica un problema de seguridad en un recurso tecnológico, debe notificarlo inmediatamente a un administrador del sistema. Los usuarios no deben demostrar el problema a otros usuarios. A cualquier usuario identificado como un riesgo de seguridad se le negará el acceso.
17. Los maestros deberán hacer esfuerzos razonables para supervisar el uso de Internet por parte de los estudiantes durante el tiempo de instrucción, para garantizar que dicho uso sea apropiado para la edad del estudiante y las circunstancias y el propósito del uso.
18. No se pueden colocar comentarios o imágenes en Internet u otros recursos tecnológicos que representen el punto de vista de la escuela o el distrito escolar sin la aprobación previa del superintendente o su designado.
19. Sin el permiso de la Junta, los usuarios no pueden conectar ninguna tecnología de propiedad personal, como computadoras portátiles y estaciones de trabajo, puntos de acceso inalámbrico y enrutadores, etc., a redes propiedad y mantenidas por el distrito. No se permite la conexión de dispositivos personales como iPods, teléfonos inteligentes, tabletas digitales e impresoras. La junta no es responsable del contenido al que acceden los usuarios que se conectan a Internet a través de la tecnología de su teléfono móvil personal (por ejemplo, servicio 3G, 4G).
20. Los usuarios deben realizar copias de seguridad de los datos y otros archivos importantes con regularidad.
21. Aquellos que usan tecnologías propiedad y mantenidas por el distrito para acceder a Internet en el hogar son responsables tanto del costo como de la configuración de dicho uso.
22. Los estudiantes a quienes se les entreguen computadoras portátiles de propiedad y mantenidas por el distrito también deben seguir estas pautas:
 - a. Mantenga la computadora portátil segura y libre de daños.
 - b. Utilice en todo momento el estuche protector tipo mochila provisto.
 - c. No preste la computadora portátil, el cargador o los cables.
 - d. No deje la computadora portátil en su vehículo.
 - e. No deje la computadora portátil desatendida.
 - f. No coma ni beba mientras usa la computadora portátil ni tenga alimentos o bebidas cerca de la computadora portátil.
 - g. No permita que las mascotas se acerquen a la computadora portátil.
 - h. No coloque la computadora portátil en el piso o en un área para sentarse, como una silla o un sofá.
 - i. No deje la computadora portátil cerca de los bordes de la mesa o del escritorio.
 - j. No apile objetos encima de la computadora portátil.
 - k. No deje la computadora portátil afuera.
 - l. No utilice la computadora portátil cerca del agua, como una piscina.
 - m. No despache el portátil como equipaje en el aeropuerto.
 - n. **Realice copias de seguridad de los datos y otros archivos importantes con regularidad. El Distrito Escolar de Corinth en ocasiones realizará el mantenimiento de las computadoras portátiles mediante imágenes y otros servicios relacionados con el apoyo. Todos los archivos que no estén respaldados en un dispositivo de almacenamiento se eliminarán durante este proceso. Mantenga una copia de seguridad personal de todos los archivos para la recuperación de datos.**

B. MATERIAL RESTRINGIDO EN INTERNET

Internet y las comunicaciones electrónicas ofrecen entornos fluidos en los que los estudiantes pueden acceder o estar expuestos a materiales e información de diversas fuentes que cambian rápidamente, incluidas algunas que pueden ser perjudiciales para los estudiantes. La Junta reconoce que es imposible predecir con certeza a qué información en Internet pueden acceder u obtener los estudiantes. No obstante, el personal del distrito escolar deberá tomar precauciones razonables para evitar que los estudiantes accedan a material e información que sea obsceno, pornográfico o de otra manera dañino para los menores, incluida la violencia, la desnudez o el lenguaje gráfico que no tenga un propósito pedagógico legítimo. El superintendente se asegurará de que las medidas de protección tecnológica se utilicen y se deshabiliten o minimicen solo cuando lo permita la ley y la política de la junta. La junta no es responsable del contenido al que acceden los usuarios que se conectan a Internet a través de la tecnología de su teléfono móvil personal (por ejemplo, servicio 3G, 4G).

C. CONSENTIMIENTO DE LOS PADRES

La junta reconoce que los padres de menores son responsables de establecer y transmitir los estándares que sus hijos deben seguir al usar los medios y las fuentes de información. En consecuencia, antes de que un estudiante pueda acceder a Internet de forma independiente, el padre o tutor del estudiante debe ser consciente de la posibilidad de que el estudiante obtenga acceso a material inapropiado mientras utiliza Internet de forma independiente. El padre y el estudiante deben dar su consentimiento para que el estudiante tenga acceso independiente a Internet y para que el personal de la escuela controle la comunicación por correo electrónico del estudiante. Además, de acuerdo con las metas y visiones de la junta para la tecnología, los estudiantes pueden requerir cuentas en sistemas de terceros para proyectos relacionados con la escuela diseñados para ayudar a los estudiantes a dominar comunicaciones en línea efectivas y adecuadas o para alcanzar otras metas educativas. Se obtendrá el permiso de los padres cuando sea necesario para crear y administrar dichas cuentas de terceros.

D. PRIVACIDAD

No existe derecho a la privacidad en el uso de los recursos tecnológicos. Los usuarios no deben asumir que los archivos o las comunicaciones a los que se acceda, descargue, cree o transmita utilizando los recursos tecnológicos del distrito escolar o que se almacenen en servicios o discos duros de computadoras individuales serán privados. Los administradores del distrito escolar o las personas designadas por el superintendente pueden revisar archivos, controlar todas las comunicaciones e interceptar mensajes de correo electrónico para mantener la integridad del sistema y garantizar el cumplimiento de la política de la junta y las leyes y reglamentos aplicables. El personal del distrito escolar deberá monitorear las actividades en línea de las personas que acceden a Internet a través de una computadora propiedad de la escuela o un equipo propiedad del distrito. En determinadas circunstancias, es posible que se requiera que la junta divulgue dicha información electrónica a las fuerzas del orden u otros terceros, por ejemplo, como respuesta a una solicitud de producción de documentos en una demanda contra la junta, como respuesta a una solicitud de registros públicos o como evidencia de actividad ilegal en una investigación criminal.

E. SEGURIDAD/CAUIDADO DE LA PROPIEDAD

La seguridad en cualquier sistema informático es de alta prioridad, especialmente cuando el sistema involucra a muchos usuarios. Los empleados son responsables de informar las violaciones de seguridad de la información al personal apropiado. Los empleados no deben demostrar la supuesta violación de seguridad a otros usuarios. Los intentos no autorizados de iniciar sesión en cualquier computadora del sistema escolar en la red de la junta como administrador del sistema pueden resultar en la cancelación de los privilegios de usuario y/o acción disciplinaria adicional. A cualquier usuario identificado como un riesgo de seguridad o que tenga un historial de problemas con otros sistemas se le puede negar el acceso. Se espera que los usuarios de los recursos tecnológicos del distrito escolar respeten la propiedad del distrito escolar y sean responsables en el uso del equipo. Los usuarios deben seguir todas las instrucciones relacionadas con el mantenimiento o el cuidado del equipo. Los usuarios pueden ser considerados responsables por cualquier pérdida o daño causado por actos intencionales o negligentes en el cuidado de las computadoras mientras están bajo su control. El distrito escolar es responsable de cualquier mantenimiento de rutina o reparación estándar de las computadoras del sistema escolar.

F. SITIOS WEB PERSONALES/REDES SOCIALES

El distrito reconoce el uso de las redes sociales en línea como una herramienta de comunicación y aprendizaje electrónico. Como resultado, el distrito proporciona herramientas sociales innovadoras protegidas con contraseña para fines de aprendizaje electrónico y colaboración. Sin embargo, las redes sociales públicas no se pueden usar para la instrucción en el salón de clases sin el consentimiento previo del superintendente. Se prohíbe el uso de las redes sociales para uso personal durante el tiempo del distrito (en contrato). El distrito puede usar las redes sociales disponibles públicamente para cumplir con su responsabilidad de comunicarse de manera efectiva y oportuna con el público en general, a través de empleados designados bajo la dirección de la junta.

El superintendente puede utilizar cualquier medio disponible para solicitar la eliminación de sitios web personales que interrumpan sustancialmente el entorno escolar o que utilicen nombres, logotipos o marcas registradas del distrito escolar o de escuelas individuales sin permiso.

1. Estudiantes

Aunque el personal de la escuela generalmente no supervisa la actividad de Internet de los estudiantes realizada en dispositivos que no pertenecen al distrito escolar fuera del horario escolar, cuando el comportamiento en línea del estudiante tiene un efecto directo e inmediato en la seguridad escolar o en el mantenimiento del orden y la disciplina en las escuelas, el estudiante puede ser disciplinado de acuerdo con la política de la junta.

2. Empleados

Todos los empleados deben mantener una relación profesional adecuada con los estudiantes en todo momento. Los sitios web personales de los empleados y las publicaciones, exhibiciones o comunicaciones en las redes sociales deben cumplir con todas las leyes estatales y federales y las políticas distritales aplicables, incluido el Código de ética y normas de conducta para educadores de Mississippi, que exige una conducta profesional y ética.

3. Voluntarios

Los voluntarios deben mantener una relación adecuada con los estudiantes en todo momento. Se alienta a un voluntario a impedir que los estudiantes vean información personal en los sitios web personales del voluntario o perfiles de redes en línea para evitar la posibilidad de que los estudiantes puedan ver materiales que no son apropiados para su edad. La relación de un voluntario individual con el distrito escolar puede terminarse si el voluntario participa en una interacción en línea inapropiada con los estudiantes.

G. RESPONSABILIDAD FEDERAL

El Distrito Escolar de Corinth para ser elegible para los Fondos Federales debe incorporar y cumplir con los requisitos de CIPA y COPPA en la Política de Uso Aceptable del distrito.

Ley de Protección de Niños en Internet (CIPA)

CIPA requiere que las escuelas y bibliotecas que reciben Fondos Federales específicos certifiquen a la agencia de financiación que cuentan con una Política de Seguridad en Internet. Tal política debe usar tecnología que bloquee el acceso a obscenidades, pornografía infantil o material dañino para menores. También puede incluir el seguimiento de los niños mientras están en línea. El Congreso quiere que la Política de seguridad en Internet aborde la piratería, las salas de chat, la seguridad del correo electrónico, la divulgación de información personal sobre niños y las actividades ilegales de niños en línea. CIPA entró en vigencia el 21 de abril de 2001. Además, el Distrito Escolar de Corinth, de acuerdo con la Ley de mejora de datos de banda ancha (BDIA) de 2008, está implementando una política que aborda el acoso cibernético y otros problemas de redes sociales.

Ley de Mejora de Datos de Banda Ancha (BDIA)

BDIA declara que el problema de la seguridad en Internet incluye problemas relacionados con el uso de Internet de una manera que promueva la actividad en línea segura para los niños, proteja a los niños de los delitos cibernéticos, incluidos los delitos cometidos por depredadores en línea, y ayude a los padres a proteger sus hijos de material inapropiado para menores. BDIA modifica la Ley de Comunicaciones de 1934 para exigir que las escuelas primarias y secundarias con acceso a computadoras a Internet eduquen a los menores sobre el comportamiento en línea apropiado, incluida la interacción en línea con otras personas en los sitios web de redes sociales y en las salas de chat y la concientización y respuesta al acoso cibernético.

H. EXENCIÓN

La junta no ofrece garantías de ningún tipo, ya sean expresas o implícitas, por el servicio que brinda. La junta no será responsable de los daños sufridos por cualquier usuario. Dichos daños incluyen, pero no se limitan a, la pérdida de datos resultante de retrasos, falta de entrega o interrupciones del servicio, ya sea causado por negligencia, errores u omisiones del distrito escolar o del usuario. El uso de cualquier información obtenida a través de Internet es bajo el propio riesgo del usuario. El distrito escolar renuncia específicamente a cualquier responsabilidad por la precisión o calidad de la información obtenida a través de sus servicios de Internet.

Solicitud/Contrato de Usuario: Certifico que he leído la Política de Uso Aceptable (AUP) del Distrito Escolar de Corinth. Entiendo y acepto seguir los Términos y condiciones anteriores para el uso de Internet del Distrito. Entiendo que cualquier violación de la AUP de Internet del Distrito resultará en la pérdida del acceso a Internet y/o mi cuenta de usuario; puede resultar en la pérdida de dispositivos tecnológicos proporcionados por la escuela; puede resultar en otra acción disciplinaria; y puede constituir un delito penal. Acepto informar cualquier uso indebido de los recursos de Internet al administrador de mi sistema. Uso Internet bajo mi propio riesgo y por la presente libero al Distrito de cualquier reclamo que surja de mi uso de Internet. *Nota: Este acuerdo se colocará en el archivo permanente del usuario.*

Nombre de usuario (letra de imprenta): _____

Firma de usuario: _____ Fecha: _____

PADRE o TUTOR: Como padre o tutor de este estudiante, he leído la Política de Uso Aceptable (AUP) del Distrito y este contrato. Entiendo que el acceso a los recursos de Internet está diseñado con fines educativos. Entiendo que hay material controvertido disponible en Internet y permito que mi hijo use Internet a pesar de esta posible disponibilidad. No responsabilizaré al Distrito por los materiales que mi hijo adquiera en la red. Mi hijo usa Internet bajo su propio riesgo y bajo mi propio riesgo. Por la presente libero al Distrito de cualquier reclamo que surja del uso de Internet por parte de mi hijo. Acepto informar cualquier uso indebido de los recursos de Internet a un administrador del Distrito. Acepto toda la responsabilidad de la supervisión siempre y cuando el uso de mi hijo no sea en un entorno escolar. Entiendo que la violación de mi hijo de la AUP de Internet del Distrito resultará en la pérdida del acceso a Internet y/o la cuenta de usuario de mi hijo; puede resultar en la pérdida de dispositivos tecnológicos provistos por la escuela; puede resultar en otra acción disciplinaria; y puede constituir un delito penal. Por la presente doy mi permiso para que mi hijo acceda a Internet y doy permiso al Distrito para que emita una cuenta para mi hijo. Certifico que la información contenida en esta solicitud es correcta.

Nombre del padre/tutor (letra de imprenta): _____

Firma del padre/tutor: _____ Fecha: _____

TENGA EN CUENTA: Aunque la política del distrito prohíbe que los usuarios no autorizados accedan a Internet; el Distrito no puede garantizar que los estudiantes no obtengan acceso no autorizado. El Distrito no es responsable por dicho acceso no autorizado.
