Procedimiento de uso aceptable por tecnología

Escuelas del condado de Overton

Este procedimiento se revisará formalmente al menos dos veces al año y se actualizará según sea necesario para garantizar el cumplimiento de la ley de Tennessee.

Última reseña: mayo de 2026

Las Escuelas del Condado de Overton reconocen que el uso efectivo de la tecnología mejora la calidad educativa al permitir el acceso a fuentes únicas de información y al proporcionar oportunidades significativas para el trabajo colaborativo. Este procedimiento establece estándares para el uso aceptable de la tecnología por parte de estudiantes, personal y visitantes. Los anexos a este procedimiento proporcionan mecanismos para implementar diversas secciones. Este procedimiento cumple con todas las leyes federales y estatales aplicables de Tennessee sobre seguridad en internet para estudiantes, incluyendo los requisitos de políticas de uso aceptable, filtrado de contenido, monitorización y notificación a los padres bajo el Código de Tennessee Anotado Título 49.

1. Definiciones

- Un estudiante es cualquier persona inscrita en una clase en cualquier instalación de las Escuelas del Condado de Overton.
- Un miembro del personal es cualquier empleado de las Escuelas del Condado de Overton o cualquier contratista empleado por una empresa que preste servicios remunerados al distrito.
- Un Visitante es cualquier persona que no emplea y accede a recursos tecnológicos dentro de cualquier instalación propiedad o utilizada por las Escuelas del Condado de Overton.
- Un padre es un padre o madre natural o adoptivo, o cualquier persona que actúe en calidad de padre. Usuarios se refiere colectivamente a Estudiantes, Personal y Visitantes.

- Un recurso tecnológico incluye cualquier red local o de área amplia, circuito de telecomunicaciones, cableado o inalámbrico, utilizado para acceder a Internet o a cualquier fuente de información, así como cualquier dispositivo informático.
- Una cuenta se refiere a cualquier cuenta de Azure Active Directory u otro conjunto de credenciales utilizado para autenticar a un usuario y acceder a recursos tecnológicos del distrito.

2. Políticas generales

El uso de recursos tecnológicos es un privilegio sujeto a todas las leyes y políticas del distrito aplicables. Los usuarios son responsables del uso ético y educativo de la tecnología del distrito. La persona para la que se crea una cuenta es responsable de todas las actividades asociadas a esa cuenta.

No se espera privacidad al utilizar los recursos tecnológicos de las Escuelas del Condado de Overton. Toda la información procesada, creada o transmitida a través de los sistemas distritales está sujeta a las leyes de registros públicos. El distrito puede examinar la información en cualquier momento, con o sin conocimiento del usuario, ya sea en tiempo real o mediante revisión histórica.

La monitorización puede realizarse cuando sea necesario para acceder a información durante la ausencia del usuario, diagnosticar problemas técnicos, realizar mantenimiento, recopilar información para litigios, apoyar auditorías, investigar infracciones sospechosas, cumplir con los requisitos legales o responder a solicitudes de la Ley de Registros Abiertos. Las supuestas infracciones que involucren a empleados deberán ser reportadas al director o jefe de departamento correspondiente e investigadas con la participación del Departamento de Tecnología de la Información. Las infracciones claras y deliberadas pueden conllevar acciones disciplinarias hasta el despido, y pueden iniciarse acciones penales o civiles cuando sea apropiado.

Los padres o tutores deben ser notificados cuando un estudiante menor de dieciocho años accede a contenido utilizando internet proporcionado por la escuela que viole este procedimiento. La notificación se realizará de manera oportuna utilizando métodos de comunicación aprobados por el distrito.

3. Seguridad de los datos y cumplimiento de derechos de autor

Los usuarios deben entender que las comunicaciones electrónicas pueden ser reenviadas, interceptadas, impresas o almacenadas por terceros, incluso cuando utilizan sistemas distritales. Las comunicaciones eliminadas aún pueden ser recuperables. Los usuarios deben evitar almacenar información personal confidencial en los recursos del distrito.

Todos los usuarios deben cumplir con las leyes de derechos de autor. Está prohibida la transmisión de material protegido por derechos de autor, confidencial, amenazante, obsceno o ilegal. Los usuarios solo pueden acceder a material protegido por derechos de autor para investigación conforme a los acuerdos publicados y la legislación aplicable.

El distrito garantizará que los estudiantes no puedan acceder a solicitudes o servicios que no protejan adecuadamente la información personal de los estudiantes contra el uso o divulgación no autorizados.

4. Filtrado de red

Las Escuelas del Condado de Overton llevan a cabo esfuerzos de buena fe para filtrar contenidos inaceptables. A pesar de estos esfuerzos, el contenido objetable puede seguir siendo accesible debido a intentos de elusión o a contenido recién creado que aún no ha sido identificado por el software de filtrado. El acceso de los estudiantes puede limitarse a sitios web, solicitudes y servicios **aprobados por el distrito** para uso educativo.

Los sistemas de filtrado deben impedir el acceso a:

- Material pornográfico u obsceno
- Contenido excesivamente violento o aterrador, inapropiado para la edad o madurez
- Contenido sin valor educativo legítimo
- Contenido que promueve la autolesión o conductas inseguras

Todos los materiales y servicios didácticos digitales deben:

- Incluir salvaguardas contra contenido dañino o inapropiado

- Cumple con las protecciones de privacidad de datos de los estudiantes
- Proporcionar mecanismos para la eliminación de contenido inapropiado

El distrito mantendrá un proceso para informar y resolver preocupaciones sobre el contenido digital.

5. Aplicación de leyes y políticas externas

El distrito aplica directrices de uso aceptable y acceso filtrado conforme a la ley federal, incluyendo la CIPA (47 USC §254(h)). El distrito coopera plenamente con las fuerzas del orden en investigaciones relacionadas con delitos informáticos. Las violaciones de la ley estatal o federal, incluido el Capítulo 39 del Código de Tennessee, pueden conllevar procesos penales y acciones disciplinarias por distrito.

6. Uso inaceptable

El uso inaceptable incluye actividades ilegales como violar leyes de derechos de autor, descargar software sin licencia, instalar virus, hackear o usar software de intercambio de archivos. Incluye acceder o transmitir material amenazante, obsceno, pornográfico, profano, discriminatorio o de otro tipo inapropiado. Incluye transmitir declaraciones incendiarias, participar en actividades políticas, intentar eludir la seguridad, usar contraseñas administrativas sin autorización, descargar medios piratas, acceder a sitios no curriculares o dañinos, vandalizar equipos o datos, causar congestión en la red, malgastar recursos, obtener acceso no autorizado, revelar información personal, invadir la privacidad, usar las credenciales de otro usuario, participar en actividades no autorizadas, publicar de forma anónima o ilegal mensajes, acoso, falsificación de identificaciones, modificación de datos de otros o introducción consciente de virus.

7. Etiqueta en redes y emisión de contactos

Los usuarios deben ser educados y usar un lenguaje apropiado. No se deben revelar datos personales. Los usuarios deben recordar que otros pueden tener diferentes orígenes culturales o lingüísticos. El reenvío de correos electrónicos solo debe hacerse en condiciones de necesidad de saberlo. Están prohibidas las cartas en cadena, el spam, los anuncios y las solicitudes no autorizadas. El correo electrónico es solo para uso educativo o administrativo y puede ser monitorizado en cualquier momento. Todo el contenido del correo electrónico es propiedad del distrito.

Las firmas de correo electrónico deben mantenerse profesionales e incluir logotipos del distrito, el nombre del empleado, el puesto de trabajo, la dirección, números de teléfono, dirección de correo electrónico, ubicación de la oficina o aula, información de contacto del colegio, iconos o enlaces del distrito o del colegio, una foto profesional, la declaración de misión del distrito o una declaración de confidencialidad. No se permiten otros objetos, incluidas citas o imágenes personales.

8. Renuncia a la responsabilidad

Las Escuelas del Condado de Overton no ofrecen garantías respecto a la funcionalidad o fiabilidad de sus servicios tecnológicos. El distrito no se hace responsable de la pérdida de datos, interrupciones del servicio, asesoramiento externo, obligaciones financieras contraídas por los usuarios ni comunicaciones realizadas por individuos que utilizan los sistemas del distrito. El distrito intentará filtrar los correos electrónicos de estafa, pero no se hace responsable de las pérdidas derivadas de estafas.

9. Políticas específicas para estudiantes

Estas políticas complementan las expectativas generales y detallan las responsabilidades de los estudiantes al utilizar la tecnología del distrito. El distrito hará esfuerzos de buena fe para filtrar el material objetable, aunque el filtrado puede no ser completamente efectivo.

Las supuestas infracciones del alumnado deberán ser reportadas al profesor supervisor y luego al director, que investigará con la intervención de TI. Las violaciones confirmadas pueden conllevar sanciones como la suspensión o pérdida permanente de privilegios y acciones disciplinarias conforme al Código de Conducta Estudiantil. El uso ilegal será denunciado a las autoridades.

La tecnología personal y el uso personal de redes sociales están prohibidos sin la aprobación expresa de la instrucción. Los estudiantes no pueden publicar ni transmitir ningún material que identifique a los estudiantes ni que divulgue información protegida por FERPA.

Los estudiantes deben utilizar la tecnología solo cuando se les supervise o se les permita, informar de contenido inapropiado, reportar problemas de seguridad y abstenerse de alterar datos o configuraciones sin autorización. Los intentos de eludir filtrados o de seguridad se consideran vandalismo.

A los estudiantes de Pre-K a 8º curso se les pueden asignar cuentas únicamente para fines de identificación del sistema. Estas cuentas **no se utilizarán para enviar ni recibir comunicaciones por correo electrónico.**

10. Políticas específicas del personal

El personal debe proteger los nombres de usuario y contraseñas asignados y reportar inmediatamente cualquier posible compromiso sospechoso. El personal debe cumplir con los requisitos de CIPA, incluyendo instrucción sobre comportamiento adecuado en línea, interacciones en redes sociales y concienciación sobre el ciberacoso.

El acceso no autorizado, el hackeo o la manipulación de los sistemas de información de los estudiantes está prohibido y puede violar la FERPA. El personal debe aplicar criterios de idoneidad educativa al gestionar el acceso a bases de datos o servicios en línea. Los contratistas y consultores están sujetos a las mismas normas, con restricciones adicionales al acceder a información confidencial.

El uso personal de redes sociales se limita al tiempo libre de impuestos. Los empleados no pueden publicar material que identifique a los estudiantes ni que divulgue información confidencial. Los empleados deben renunciar a opiniones personales al publicar externamente.

Los recursos tecnológicos solo pueden utilizarse para el aprendizaje, la enseñanza y fines administrativos de acuerdo con los objetivos del distrito. Se prohíbe el uso comercial. El incumplimiento puede resultar en la revocación de privilegios y acciones disciplinarias.

La educación sobre seguridad en Internet deberá integrarse en los programas de instrucción e incluir:

- Comportamiento seguro en línea
- Interacción en plataformas digitales
- Concienciación sobre el ciberacoso
- Protección de la información personal

11. Aprendizaje a distancia

Durante la enseñanza a distancia, todos los procedimientos de uso aceptables permanecen en vigor. Los sistemas en la nube de distrito permanecen protegidos por las

políticas del distrito independientemente de la ubicación del usuario. Los usuarios deben seguir todos los procedimientos como si operaran en propiedad del distrito.

12. Auditoría y cumplimiento

Las Escuelas del Condado de Overton deberán realizar una auditoría anual para comprobar el cumplimiento de este procedimiento. La auditoría puede ser realizada por un tercero cualificado o satisfecho mediante una auditoría E-Rate cualificada. Los resultados de la auditoría se publicarán en la página web del distrito.

El distrito mantendrá procedimientos para comunicarse con los padres respecto a:

- Riesgos para la seguridad en Internet
- Salvaguardas del distrito
- Prácticas seguras de uso de tecnología

13. Referencias y Autoridad

Este procedimiento está respaldado por la Ley de Protección de Internet para Niños (47 USC §254(h)(1)), la Ley de Derechos y Privacidad Educativa Familiar (20 USCA §1232(G)), el Código de Tennessee §§3914602 y 3914105, 17 USCA §§107 y 117, la Ley de Mejora de Datos de Banda Ancha y el Código de Conducta Estudiantil de las Escuelas del Condado de Overton.