

RECURSOS ELECTRÓNICOS Y SEGURIDAD DE INTERNET

Guías aceptable/requisitos de seguridad en Internet

Estos procedimientos están escritos para respaldar la Política de Recursos Electrónicos de la Junta Directiva del Distrito Escolar de Eastmont y para promover una ciudadanía digital positiva y efectiva entre los estudiantes y el personal. La ciudadanía digital incluye las normas de comportamiento adecuado, responsable y saludable relacionadas con el uso actual de la tecnología. Los ciudadanos digitales exitosos y con fluidez tecnológica reconocen y valoran los derechos, responsabilidades y oportunidades de vivir, aprender y trabajar en un mundo digital interconectado. Cultivan y gestionan su identidad y reputación digital, y son conscientes de la permanencia de sus acciones en el mundo digital. Las expectativas sobre el comportamiento de los estudiantes y el personal en línea no son diferentes de las interacciones cara a cara.

Formulario de autorización de usuario individual

Todos los usuarios deben tener un Formulario de autorización de usuario individual firmado antes de que se les permita el acceso a los recursos de la red del Distrito. El personal debe completar y enviar el formulario 2022-F1 al momento de la contratación. Los estudiantes deben completar 2022-F2 al momento de registrarse para asistir a la escuela en el Distrito. Los estudiantes menores de 18 años deben tener la aprobación de un padre/tutor.

Uso de dispositivos electrónicos personales

De acuerdo con todas las políticas y procedimientos del Distrito Escolar de Eastmont, los estudiantes y el personal reciben dispositivos del Distrito para promover la misión educativa del Distrito. La administración escolar conservará la autoridad final para decidir cuándo y cómo los estudiantes pueden usar dispositivos electrónicos personales en los terrenos escolares y durante el día escolar. En ausencia de una necesidad específica y articulada (por ejemplo, tecnología de asistencia), los estudiantes no tienen el derecho absoluto de poseer o usar dispositivos electrónicos personales en la escuela.

- A. Se requiere que los estudiantes utilicen un dispositivo emitido por el Distrito Escolar de Eastmont para acceder al contenido digital y al plan de estudios mientras están en la escuela o fuera de ella.
- B. No se permiten computadoras portátiles/computadoras/tabletas personales en la escuela.
 - 1. Los dispositivos personales podrían eludir los servicios de monitoreo de seguridad de los estudiantes (p. ej., Gaggle), el monitoreo/administración del aula (p. ej., Impero Classroom) y, potencialmente, el filtrado web.
 - 2. La administración del edificio puede otorgar excepciones para dispositivos personales que requieren acceso Wifi y todas las partes deben completar y firmar el formulario 2022-F3.

C. El uso de teléfonos celulares debe seguir la Política de la Junta Escolar No. 3245 [Estudiantes y dispositivos de telecomunicaciones](#).

El Network/ La red

La red del Distrito incluye dispositivos y equipos periféricos cableados e inalámbricos, archivos y almacenamiento, correo electrónico y contenido de Internet (blogs, sitios web, software de colaboración, sitios de redes sociales, wikis, etc.). El Distrito se reserva el derecho de priorizar el uso y el acceso a la red.

Todo uso de la red debe apoyar la educación y ser consistente con la misión del Distrito.

El uso aceptable de los recursos tecnológicos del Distrito por parte del personal y los estudiantes del Distrito incluye:

- A. Creación de archivos, proyectos digitales, vídeos, páginas web y podcasts utilizando recursos de la red en apoyo de la educación y la investigación;
- B. Participación aprobada y supervisada por el distrito en sitios web que apoyan la educación y la investigación;
- C. Con permiso de los padres, la publicación en línea de material educativo original, materiales relacionados con el plan de estudios y trabajos de los estudiantes. Se deben citar adecuadamente las fuentes fuera del aula o de la escuela; y
- D. Uso de la red por parte del personal para uso personal incidental de acuerdo con todas las políticas y procedimientos del Distrito..

El uso inaceptable de la red por parte del personal y los estudiantes del Distrito incluye, entre otros:

- A. La línea de guía general de Eastmont tanto para el personal como para los estudiantes utiliza tecnología antigua: la prueba del periódico. Esto significa preguntar mientras usan la tecnología del Distrito si les gustaría que lo que están escribiendo, viendo o escuchando aparezca en la portada del Wenatchee World Newspaper (o en una versión en línea). Si no, entonces deberían parar inmediatamente. Si hay dudas sobre el uso, deben pedir orientación a un supervisor sobre el uso apropiado;
- B. Ganancia personal, solicitud comercial y compensación de cualquier tipo;
- C. Acceder al correo electrónico personal u otras cuentas personales desde un dispositivo propiedad del Distrito;
- D. Iniciar sesión o utilizar la cuenta de otra persona de cualquier forma;
- E. Acciones que resulten en responsabilidad o costos incurridos por el Distrito;
- F. Los usuarios sólo deberán utilizar software con licencia y actualizado. Cualquier instalación debe ser completada por un miembro del personal de tecnología del Distrito u otra persona aprobada.
- G. Apoyo u oposición a medidas electorales, candidatos y cualquier otra actividad política;
- H. El pirateo, el craqueo, el vandalismo y la introducción de malware incluyen virus,

- gusanos, caballos de Troya, bombas de tiempo y cambios en el hardware, el software y las herramientas de supervisión;
- I. Acceso no autorizado a otras computadoras, redes y sistemas de información del Distrito;
 - J. Acción que constituya acoso, intimidación o acoso, incluido el acoso cibernético, correo de odio, difamación, bromas y comentarios discriminatorios. Esto también puede incluir la fabricación, distribución o posesión de imágenes digitales inapropiadas;
 - K. Información publicada, enviada o almacenada en línea que podría poner en peligro a otros (por ejemplo, construcción de bombas, fabricación de drogas);
 - L. Abrir correos electrónicos o archivos adjuntos de orígenes desconocidos;
 - M. Enviar por correo electrónico o compartir software u otro material protegido por derechos de autor u otra violación de las leyes de derechos de autor;
 - N. Se prohíbe la instalación, el uso, el almacenamiento o la distribución no autorizados de software o materiales protegidos por derechos de autor;
 - O. Acceder, cargar, descargar, almacenar y distribuir material obsceno, pornográfico o sexualmente explícito;
 - P. Conectar dispositivos no autorizados a la red del Distrito. Cualquier dispositivo de este tipo será confiscado y se podrán tomar medidas disciplinarias adicionales;
 - Q. Cualquier uso ilegal de la red del Distrito, incluidos, entre otros, acecho, chantaje y fraude; o
 - R. Cualquier actividad que interrumpa las actividades escolares o del distrito..

El Distrito no será responsable de ningún daño sufrido por ningún usuario, incluyendo, entre otros, pérdida de datos resultante de retrasos, falta de entrega, entregas erróneas o interrupciones del servicio causadas por su propia negligencia o cualquier otro error. u omisiones. El Distrito no será responsable de las obligaciones financieras no autorizadas que resulten del uso o acceso a la red informática del Distrito o Internet.

Seguridad en Internet/Información personal y contenido inapropiado

- A. El personal y los estudiantes no deben revelar información personal, incluida la dirección particular y el número de teléfono, en sitios web, blogs, podcasts, videos, sitios de redes sociales, wikis, correos electrónicos o como contenido en cualquier otro medio electrónico;
- B. El personal y los estudiantes no deben revelar información personal sobre otra persona en ningún medio electrónico sin obtener permiso primero;
- C. Las fotografías o los nombres de los estudiantes no se pueden publicar en ninguna clase pública, escuela o sitio web del Distrito a menos que se haya obtenido el permiso correspondiente de acuerdo con el Formulario 2022-F2;
- D. Si los estudiantes encuentran información o mensajes peligrosos o inapropiados, deben notificar a la autoridad escolar correspondiente de inmediato; y
- E. Los estudiantes deben ser conscientes de la persistencia de su información digital, incluidas imágenes y actividad en las redes sociales, que pueden permanecer en Internet indefinidamente.

Filtrado y Monitoreo

El software de filtrado se utiliza para bloquear o filtrar el acceso a representaciones visuales obscenas y a toda la pornografía infantil de acuerdo con la [Ley de Protección Infantil en Internet \(CIPA\)](#). Se podría filtrar otro material objetable.

- A. El software de filtrado no es 100 por ciento efectivo. Si bien los filtros dificultan la recepción o el acceso a material objetable, no son una solución en sí mismos. Todo usuario debe asumir la responsabilidad del uso que hace de la red e Internet y evitar sitios objetables;
- B. Se prohíbe cualquier intento de derrotar o eludir el filtro de Internet del Distrito u ocultar la actividad de Internet (por ejemplo, servidores proxy, https, puertos especiales, modificaciones a la configuración del navegador del Distrito y cualquier otra técnica diseñada para evadir el filtrado o permitir la publicación de contenido inapropiado);
- C. Los correos electrónicos que no sean coherentes con la misión educativa y de investigación del Distrito se considerarán SPAM y se bloqueará su entrada a los buzones de correo electrónico del Distrito;
- D. El Distrito proporcionará supervisión adulta adecuada del uso de Internet. La primera línea de defensa para controlar el acceso de menores a material inapropiado en Internet es el monitoreo deliberado y consistente del acceso de los estudiantes a los dispositivos del Distrito;
- E. Los miembros del personal que supervisan a los estudiantes, controlan equipos electrónicos o tienen la oportunidad de observar el uso de dichos equipos por parte de los estudiantes en línea, deben hacer un esfuerzo razonable para monitorear el uso de este equipo para garantizar que el uso de los estudiantes se ajuste a la misión y los objetivos del Distrito.
- F. El personal debe hacer un esfuerzo razonable para familiarizarse con Internet y monitorear, instruir y ayudar de manera efectiva;
- G. El Distrito puede monitorear el uso de la red del Distrito por parte de los estudiantes, incluso cuando se accede a ellos desde dispositivos electrónicos personales de los estudiantes y dispositivos proporcionados por el Distrito, como computadoras portátiles, Chromebooks y tabletas; y
- H. El Distrito proporcionará un procedimiento para que el personal solicite acceso a sitios web de Internet bloqueados por el software de filtrado del Distrito. Los requisitos del "Formulario de aprobación de tecnología educativa" cubren un amplio criterio que incluye el cumplimiento de regulaciones federales como CIPA, COPPA, FERPA. Además de una justificación de cómo el sitio web complementa la instrucción básica.

Instrucciones de seguridad en Internet

Todos los estudiantes recibirán educación sobre el comportamiento apropiado en línea, incluida la interacción con otras personas en sitios web de redes sociales y salas de chat, y la concientización y respuesta al acoso cibernético:

- A. Se pondrán a disposición materiales apropiados para la edad para su uso en todos los niveles de grado; y

- B. Se pondrá a disposición de la administración, el personal y las familias capacitación sobre cuestiones de seguridad en línea e implementación de materiales.

Derechos de autor

Por lo general, está prohibido descargar, copiar, duplicar y distribuir software, música, archivos de sonido, películas, imágenes u otros materiales protegidos por derechos de autor sin el permiso específico por escrito del propietario de los derechos de autor.

Todo uso de cualquier material que no sea el plan de estudios aprobado en el aula es responsabilidad del miembro del personal individual de verificar que se sigan las guías de derechos de autor en duplicación y distribución. Los miembros del personal deben estar preparados para respaldar todas las acciones de duplicación y distribución de material externo a la Administración del Distrito tras la notificación.

Servicios de transmisión de vídeo

Los servicios de streaming (Netflix, Disney+, Amazon Prime, Hulu, etc.) están bloqueados en la red de Eastmont. Los términos de servicio que uno acepta al comprar el servicio de transmisión pago son solo para uso personal, no deben usarse en un lugar público, incluido un salón de clases, y constituirían una violación de esos términos de servicio.

Propiedad del trabajo

Todo el trabajo realizado por los empleados como parte de su empleo se considerará propiedad del Distrito. El Distrito será propietario de todos y cada uno de los derechos sobre dicho trabajo, incluidos todos y cada uno de los trabajos derivados, a menos que exista un acuerdo escrito en contrario.

Todo el trabajo completado por los estudiantes como parte del programa de instrucción regular es propiedad del estudiante tan pronto como se crea, a menos que dicho trabajo se cree mientras el estudiante actúa como empleado del sistema escolar o a menos que dicho trabajo haya sido pagado según un acuerdo escrito con el sistema escolar. Si está bajo acuerdo con el Distrito, la obra se considerará propiedad del Distrito. El personal debe obtener el permiso del estudiante antes de distribuir su trabajo a fiestas fuera de la escuela.

Seguridad y privacidad de la red

Las contraseñas son el primer nivel de seguridad para una cuenta de usuario. Los inicios de sesión y las cuentas del sistema deben ser utilizados únicamente por el propietario autorizado de la cuenta para fines autorizados del Distrito. El personal y los estudiantes son responsables de toda la actividad en su cuenta y no deben compartir la contraseña de su cuenta ni dejar un archivo o sesión abiertos sin supervisión. Los propietarios de cuentas son, en última instancia, responsables de toda la actividad realizada en su cuenta.

Los siguientes procedimientos están diseñados para proteger las cuentas de usuarios de la red:

- A. Cambiar contraseñas de acuerdo con la política del Distrito;
- B. No utilice la cuenta de otro usuario;
- C. No inserte contraseñas en correos electrónicos u otras comunicaciones;
- D. Si anota la contraseña de su cuenta de usuario, guárdela en un lugar seguro;
- E. No almacene contraseñas en un archivo sin cifrado;
- F. No utilice la función "recordar contraseña" de los navegadores de Internet;
- G. Notificar a los administradores de red si su información personal ha sido comprometida;
- H. Los usuarios no deberán buscar información, obtener copias, modificar archivos, datos o contraseñas que pertenezcan a otros usuarios, ni tergiversar a otros usuarios, ni intentar obtener acceso no autorizado a ningún sistema; y
- I. Bloquee la pantalla o cierre la sesión si deja una computadora.

Los datos del estudiante son confidenciales

El personal del distrito debe mantener la confidencialidad de los datos de los estudiantes de acuerdo con la [Ley de Privacidad y Derechos Educativos de la Familia \(FERPA\)](#).

Sin expectativas de privacidad

El Distrito proporciona el sistema de red, correo electrónico y acceso a Internet como herramienta para la educación y la investigación en apoyo de la misión del Distrito. El Distrito se reserva el derecho de monitorear, inspeccionar, copiar, revisar y almacenar, sin previo aviso, información sobre el contenido y el uso de:

- A. La red del Distrito, incluso cuando se accede a ella desde los dispositivos electrónicos personales de los estudiantes y en dispositivos proporcionados por el Distrito, como computadoras portátiles, netbooks y tabletas;
- B. Archivos de usuario y utilización del espacio en disco;
- C. Aplicaciones de usuario y utilización del ancho de banda;
- D. Archivos documentales, carpetas y comunicaciones electrónicas del usuario;
- E. Correo electrónico;
- F. Acceso a Internet; y
- G. Toda la información transmitida o recibida en relación con el uso de la red y el correo electrónico.

Ningún estudiante o usuario del personal debe tener expectativas de privacidad al utilizar la red del Distrito. El Distrito se reserva el derecho de revelar cualquier mensaje electrónico a funcionarios encargados de hacer cumplir la ley o a terceros, según corresponda. Todo el contenido está sujeto a las leyes de divulgación de registros públicos del estado de Washington.

Aplicaciones y programas educativos

El personal del distrito puede solicitar acceso para que los estudiantes puedan acceder o registrarse en sitios web, aplicaciones o programas que se utilizan en los Chromebooks proporcionados por el distrito. Estas aplicaciones y programas están diseñados para ayudar a facilitar las conferencias, la evaluación de los estudiantes, la comunicación y la retroalimentación entre profesores y estudiantes, entre otras cosas.

Se requiere que los estudiantes utilicen un dispositivo proporcionado por el Distrito para acceder al contenido digital y al plan de estudios, tanto en la escuela como fuera de ella.

Antes de solicitar que los estudiantes tengan acceso o se registren en aplicaciones o programas educativos, el personal revisará los “términos de uso”, los “términos de servicio” y/o la “política de privacidad” de cada aplicación o programa para asegurarse de que no comprometer la información de identificación personal, la seguridad y la privacidad de los estudiantes. El personal también notificará por escrito sobre el uso potencial de cualquier aplicación o programa educativo completando el Formulario de aprobación de tecnología educativa, incluido el propósito previsto de dicha aplicación o programa. El Formulario de Aprobación de Tecnología Instructiva debe estar firmado por el miembro del personal, su Director/Directora, el Director Ejecutivo de Enseñanza y Aprendizaje, así como el Director de Tecnología.

Una vez que un sitio web o una solicitud hayan sido revisados y aprobados mediante el Formulario de aprobación de tecnología educativa, se agregarán a una lista de sitios aprobados. Los padres/tutores no son notificados directamente de cada solicitud aprobada, pero se puede proporcionar una lista si la solicitan.

Archivo y copia de seguridad

Se realiza una copia de seguridad de toda la correspondencia electrónica del Distrito para fines de divulgación pública y recuperación ante desastres. Salvo cortes de energía o problemas técnicos intermitentes, los archivos del personal y de los estudiantes se respaldan periódicamente en los servidores del Distrito.

Acción disciplinaria

Todos los usuarios de los recursos electrónicos del Distrito deben cumplir con la política y los procedimientos del Distrito (y aceptar cumplir con las disposiciones establecidas en el acuerdo de usuario del Distrito). La violación de cualquiera de las condiciones de uso explicadas en el acuerdo de usuario del Distrito, la política de Recursos Electrónicos o en estos procedimientos podría ser motivo de acción disciplinaria, incluida la suspensión o expulsión de la escuela y la suspensión o revocación de los privilegios de acceso a la red y a la computadora.

Accesibilidad de los recursos electrónicos

La ley federal prohíbe que las personas, por motivos de discapacidad (como problemas de visión y audición), sean excluidas de la participación, se les nieguen los beneficios o

sean objeto de discriminación por parte del Distrito. Para garantizar que las personas con discapacidades tengan igual acceso a los programas, actividades y servicios del Distrito, el contenido y la funcionalidad de los sitios web asociados con el Distrito deben ser accesibles. Dichos sitios web pueden incluir, entre otros, la página de inicio del Distrito, sitios web de maestros, páginas de redes sociales operadas por el Distrito y conferencias de clases en línea.

Métodos de comunicación permitidos por el distrito de acuerdo con el Procedimiento No. 4040-P

El personal del Distrito con autoridad para crear o modificar el contenido o la funcionalidad del sitio web asociada con el Distrito tomará medidas razonables para garantizar que dicho contenido o funcionalidad sea accesible para personas con discapacidades. Cualquier miembro del personal que tenga preguntas sobre cómo cumplir con este requisito debe consultar con el Departamento de Tecnología del Distrito.

Todas las cuentas de medios digitales relacionadas con el trabajo y el Distrito deberán ser aprobadas por el supervisor del empleado. El acceso del personal a cada cuenta de redes sociales respectiva será otorgado por social@eastmont206.org después de la aprobación del administrador del edificio/departamento. Los padres/tutores también tendrán acceso a comunicaciones digitales que incluyan a sus estudiantes.

Eastmont limita a los empleados a las siguientes tecnologías de comunicación para comunicaciones relacionadas con el Distrito:

- A. El distrito aprobó/supervisó Google Gmail para correo electrónico.
- B. Chat de Google y mensajes de Webex aprobados/supervisados por el distrito para mensajes de texto iniciados por el supervisor.
- C. Teléfonos celulares proporcionados por el distrito/aplicaciones aprobadas por el distrito para enviar mensajes de texto.
- D. Cuentas de ParentSquare aprobadas/supervisadas por el distrito.
- E. Cuentas de Facebook aprobadas/supervisadas por el distrito.
- F. Cuentas de Twitter aprobadas/supervisadas por el distrito.
- G. Cuentas de YouTube aprobadas/supervisadas por el distrito.
- H. Cuentas de Instagram aprobadas/supervisadas por el distrito.
- I. Cuentas de Pinterest aprobadas/supervisadas por el distrito.
- J. Otras cuentas de redes sociales aprobadas por la Administración Ejecutiva del Distrito.
- K. La instrucción de los estudiantes o las cuentas en línea relacionadas con el aula están prohibidas debido a la Ley de Privacidad de los Derechos Educativos de la Familia (FERPA), excepto si lo aprueba el supervisor responsable y el director ejecutivo.

Cuidado de la tecnología del distrito

No se aceptará ningún equipo donado sin la aprobación previa por escrito del Director de Tecnología.

Se espera que los usuarios de la tecnología del Distrito respeten la propiedad del Distrito y sean responsables en el uso de la tecnología. Los usuarios deben seguir las instrucciones del Distrito con respecto al mantenimiento o cuidado de la tecnología. Los usuarios pueden ser considerados responsables de cualquier daño causado por actos negligentes mientras la tecnología del Distrito esté bajo su control. El Distrito es responsable de cualquier mantenimiento de rutina o reparaciones estándar de la tecnología del Distrito. Las recomendaciones para el cuidado y limpieza de la tecnología se pueden encontrar en la página web de Tecnología. Se espera que los usuarios notifiquen al Distrito sobre cualquier necesidad de servicio de manera oportuna.

La tecnología estudiantil (Chromebooks) es responsabilidad del estudiante. Si el daño se causa por negligencia, se emitirá una tarifa/multa a través de IIQ (Incident IQ). La tarifa/multa se informará al padre/tutor a través del recibo de Intouch.

Si la tecnología del Distrito se pierde, se daña o es robada mientras está bajo el control de un usuario, se espera que el usuario (o el padre/tutor responsable si el usuario es un estudiante) pague la tarifa/multa de manera oportuna. Se anima al usuario a presentar una reclamación bajo la cobertura de su seguro de propietario de vivienda para recuperar el gasto, cuando la cobertura esté disponible.

El Distrito Escolar de Eastmont no será responsable de ningún daño directo o indirecto, incidental o consecuente (incluida la pérdida de datos o información) sostenido o incurrido en relación con el uso, operación o imposibilidad de usar la red y/o dispositivos de Eastmont, violaciones de las políticas del Distrito. o reglas pueden resultar en medidas disciplinarias apropiadas que pueden incluir el despido.