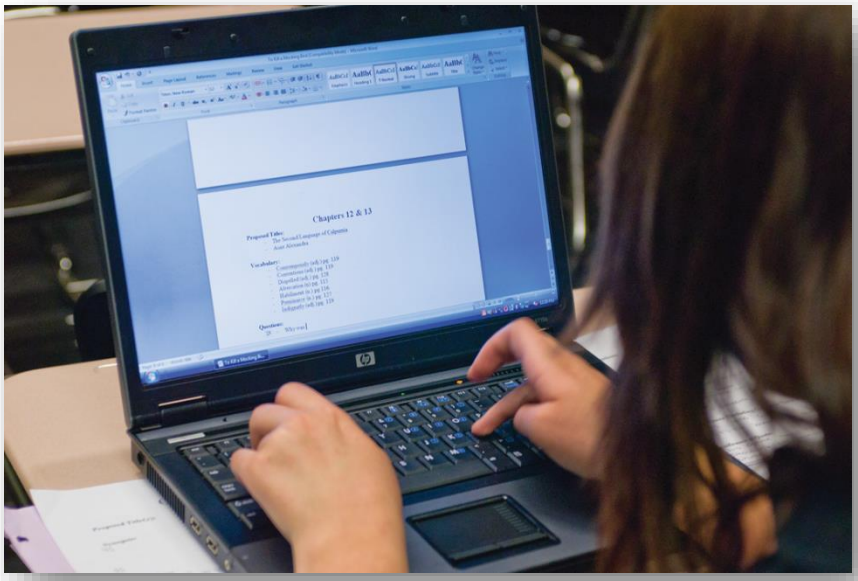

Manual de computadora portátil

Contenido

Descripción general 2
Responsabilidades del padre/tutor 2
Reglas y lineamientos para portátiles 3
Uso y cuidado de computadoras portátiles 4
Consecuencias por mal uso, pérdida o daño 5
Multas para portátiles 6
Opciones de seguro 6
Acceso a Internet 7
Políticas & procedimientos del uso de recursos electrónicos por parte del estudiante .. 7
Preguntas frecuentes (*FAQ*) 12
Recursos de seguridad en Internet 16

Acceso móvil para estudiantes de secundaria - Manual de computadora portátil

Descripción general

El acceso móvil para el programa de estudiantes permite que cada estudiante en los grados 6-12 reciban una computadora portátil o computadora *netbook* para su uso educativo, tanto en casa como en la escuela. El uso de esta herramienta está diseñado para enriquecer el ambiente de aprendizaje y ayudar a los maestros a medida que apoyan a los estudiantes en la adquisición de las competencias, conocimientos y atributos que aparecen en el perfil del estudiante del distrito.

El privilegio de acceder a la red de la escuela y a los recursos del equipo también es una oportunidad para aprender la responsabilidad del uso informado, ético y responsable de la computadora. Este manual describe muchas de estas responsabilidades. Proporciona información y recursos para las familias sobre estas expectativas.

Responsabilidades del Padre/Tutor

- Revisar las reglas y lineamientos para el portátil
- Revisar los *procedimientos de uso aceptable para estudiantes*
- Controlar el uso que el estudiante le da cuando no en la escuela
- Asegurarse de que se le da el cuidado adecuado a la computadora portátil cuando el estudiante no está en la escuela
- Determinar la opción de cobertura de seguro de su familia
- Aceptar la responsabilidad
    - Las familias son responsables por pérdidas o daños
- Firmar el acuerdo de la computadora portátil y devolverlo a la escuela

Reglas y lineamientos para portátiles

La siguiente información es un resumen de los procedimientos del Distrito de uso aceptable para estudiantes. Por favor revise el documento completo que comienza en la página 8 de este manual. Los estudiantes deben entender y seguir estos procedimientos.

- Si puede:
  - Utilizar el equipo con fines educativos
  - Utilizar el equipo en forma adecuada
  - Utilizar su buen juicio
- No debe:
  - Utilizar el equipo con fines comerciales o de lucro personal
  - Utilizarlo para fines políticos, como para tratar de influir en las elecciones
  - Utilizarlo para nada ilegal o indecente
    - Ninguna actividad ilegal, intimidación, acoso o imágenes inapropiadas
  - Utilizarlo de una forma que sea perjudicial para los demás usuarios, servicios o equipo
    - Ni spam ni virus, ni grandes cantidades de datos ni intentar piratear o violar los sistemas
- Seguridad en Internet
  - Nunca revele información personal acerca de usted o de otra persona
  - No publique imágenes o nombres de los estudiantes en ningún sitio de Internet sin permiso de la escuela
  - Si usted ve algo peligroso o inapropiado dígale a un maestro de inmediato
  - Siga la instrucción escolar acerca de la seguridad en Internet, el acoso cibernético y el buen comportamiento en línea

- Filtrado, control y seguridad de la red
  - El distrito utiliza el software de filtrado con la intención de bloquear material inapropiado u objetable
    - El software de filtrado no siempre coge el material inapropiado. Cada usuario es responsable de evitar sitios inapropiados
    - No intente eludir el filtrado, ni utilizar servidores proxy, ni puertos especiales ni cambiar la configuración del navegador
  - El uso de Internet por parte del estudiante es controlado en la escuela
  - Proteja las contraseñas:
    - Cámbielas según sea necesario
    - No comparta su contraseña ni utilice la cuenta de nadie

        - No ponga su contraseña en un mensaje de correo electrónico o de otro tipo. Si la escribe, manténgalo segura.
        - No utilice la función de "recordar contraseña" en el navegador
        - Bloquee la pantalla o cierre la sesión si deja la computadora
- Datos del estudiante y privacidad
    - El personal mantiene la confidencialidad de los datos de los estudiantes de acuerdo con la ley federal (*FERPA*). El permiso del padre o tutor es necesario para publicar trabajos de los estudiantes.
    - El uso de la red, las computadoras, la Internet y el correo electrónico del distrito no son intrínsecamente seguros ni privados. El distrito se reserva el derecho de supervisar, revisar y almacenar y/o revelar cualquier mensaje electrónico a los funcionarios encargados de hacer cumplir la ley o a terceros
    - Los documentos, incluyendo el correo electrónico, están sujetos a las leyes de divulgación de registros públicos. Se hace una copia de seguridad de toda la correspondencia de los correos electrónicos del distrito para divulgación pública y recuperación de desastres.

- Derechos de autor
    - No guarde ni copie el material con derechos de autor sin permiso del dueño, a menos que usted cumpla con la doctrina de uso justo de la ley de derechos de autor de los Estados Unidos
- Violaciones de *Procedimientos de uso aceptable para estudiantes*
    - La violación de estas reglas y pautas puede resultar en que se eliminen los privilegios de red y de la computadora. También puede significar multas por pérdidas o daños a las computadoras. La aplicación y disciplina de las reglas de conducta de la escuela pueden resultar del uso inapropiado. Usted podría ser reportado a la policía si se Involucra en una actividad ilegal. Para mayor información ver las políticas y procedimientos de disciplina del distrito para estudiantes.

Uso y cuidado de computadoras portátiles

- Lleve el dispositivo a la escuela, totalmente cargado, todos los días a menos que se indique lo contrario
- Permita siempre que un análisis del equipo o actualización complete su proceso
- No instale, desinstale ni modifique ninguna aplicación, juego o componente del sistema operativo
- No descargue emuladores de juegos, clientes de chat ni software *peer to peer*

- No coloque pegatinas ni marque la computadora. Las pegatinas o calcomanías dejan residuos en las piezas del portátil que son difíciles de eliminar. Se permiten etiquetas de identificación del tipo de "pegado" removible (*"cling" type*)
- Asegúrese que el equipo no se pierda, ni sea robado o dañado haciéndole seguimiento y cuidando los equipos:
    - No lo deje sin supervisión y siga las reglas de la escuela de seguridad cuando sea necesario, por ejemplo para actividades deportivas
    - No forzarlo para abrirlo más allá del punto de detención
    - No raye ni marque el exterior del dispositivo
    - No retire código de barras de identificación del distrito
    - No inserte objetos extraños (clips, bolígrafos) en el dispositivo
    - No coma ni beba cerca del dispositivo móvil
    - Usar sobre una superficie plana y estable
    - En el aula, la tapa del dispositivo debe estar cerrada entre los usos
    - Cuando no esté en uso, el dispositivo debe estar apagado
  - Utilice sólo los métodos adecuados de limpieza
    - No utilice agua ni soluciones de limpieza.
    - Limpie las superficies ligeramente con un paño suave y limpio.
    - Evite tocar la pantalla.

Consecuencias por mal uso, pérdida o daño

- El uso de la computadora portátil es un privilegio que puede ser revocado si se utiliza inadecuadamente o se daña.
  - Al estudiante y al padre/tutor se le cobrará por cualquier daño causado por abuso o mal uso, o la pérdida del dispositivo debido a la negligencia. Se requiere un informe policial por cualquier dispositivo robado.
- El uso inadecuado o el uso en conflicto con las reglas escolares estará de acuerdo con las políticas de disciplina de la escuela y pueden incluir:
  - La pérdida de privilegios para usar o llevar a casa la computadora personal
  - Suspensión / expulsión por infracciones graves o reiteradas
  - Otra acción correctiva
- Si el equipo se pierde o se lo roban
  - Reporte inmediatamente a la escuela acerca de los dispositivos perdidos
  - Si el dispositivo es robado, se debe presentar un informe de la policía y se debe entregar una copia a la escuela

- La pérdida o robo de un dispositivo debido a la negligencia (dejarlo sin atención, no asegurarlo de acuerdo a las reglas de la escuela) puede resultar en que deba asumir el costo total de reposición
- Si el equipo está dañado
  - Se cobrarán honorarios por daños mayores al desgaste normal, a aquellos causados por negligencia o múltiples incidentes de daños se cobrarán multas o costos de reparación/reemplazo.
  - Remitirse a la información de multas para portátiles en la página 6.

Multas para portátiles

Objetos perdidos:	Costo por reposición
Dispositivo móvil- sin devolver nada	$450.00
Batería	$55.00
Fuente de alimentación (completa con cargador y cable de alimentación	$35.00
Objetos dañados:	
Pantalla agrietada o rota	$80.00
Bisel *LCD* dañado	$45.00
Cubierta superior dañada	$80.00
Cubierta inferior dañada	$80.00
Reposamanos dañado	$80.00
Reemplazo disco duro	$70.00
Batería dañada	$55.00
Teclado dañado (reemplazo)	$70.00
Sustitución de tecla(s) que faltan	$10.00
Reemplazo tarjeta principal del sistema	$280.00
Otro _____(Costo de reparación real)	

Opciones de seguro

Las familias pueden querer protegerse contra la responsabilidad por pérdida, daño o robo de propiedad mediante la revisión de sus opciones de seguro. Algunas políticas de propietarios de vivienda pueden ofrecer cobertura y algunos pueden ofrecer esta cobertura si se adquiere una cláusula adicional. Además, *Lake Washington School District* ha dispuesto una opción de seguro para las familias que deseen adquirir un seguro específico adicional para cubrir la computadora portátil del estudiante. Este seguro se puede comprar a *Worth Insurance Group*. La prima es de $ 54.20 por año y cubre los daños accidentales y robo (se requiere informe de la policía). El deducible en esta póliza es de $0. Este seguro puede ser adquirido directamente accediendo a http://my.worthavegroup.com/lakewashington. La compañía también ofrece cobertura para otros sistemas de tecnología personal. Si opta por no comprar el seguro opcional o de otra manera no tiene

cobertura, usted será responsable de los gastos por equipos dañados o robados/perdidos como se definió anteriormente.

Acceso a Internet

¿Necesita un servicio asequible de Internet en casa? El acceso a Internet se ha convertido en algo cada vez más importante para los estudiantes para el aprendizaje en el hogar y para que las familias puedan comunicarse con la escuela. *Comcast* ofrece el servicio de Internet en casa *Internet Essentials* a las familias con estudiantes que califican para almuerzo gratis o a precio reducido y sin acceso a Internet por 90 días. Este programa ofrece un servicio de Internet en casa por $ 9.95 al mes más impuestos, sin cargos por activación, tarifas de alquiler de equipos o aumentos de precios. Una computadora de bajo costo ($ 149.99 más impuestos) está disponible en la inscripción inicial. Para obtener mayor información, visite InternetEssentials.com o llame al 1-855-846-8376.

Políticas y procedimientos del uso de recursos electrónicos por parte del estudiante

Parte de la información clave de esta política y el siguiente procedimiento se resume partir de la página 3. Por favor revise esta política y los procedimientos que siguen.

USO DE RECURSOS ELECTRÓNICOS POR PARTE DEL ESTUDIANTE

Procedimientos de uso aceptable para estudiantes (*AUP*)

Alcance
Los siguientes procedimientos se aplican a todos los estudiantes del Distrito y abarcan todos los aspectos de la red del Distrito. La red del distrito incluye computadoras/dispositivos alámbricos e inalámbricos y equipos periféricos, archivos y almacenamiento, correo electrónico y contenido de Internet y todo el software informático, aplicaciones o recursos autorizados para el Distrito.

Use apropiado de red
El Distrito espera que los estudiantes hagan uso del buen juicio y utilicen los equipos informáticos de una manera apropiada. Se espera que la utilización del equipo se relacione con fines educativos.

El uso inaceptable /prohibido de la red por parte de los estudiantes incluye:

- Uso comercial: Está prohibido el uso de la red del Distrito para beneficio personal o privado, negocios personales o ventaja comercial.
- Uso político: Está prohibido el uso de la Red del Distrito para fines políticos en violación de las leyes federales, estatales o locales. Esta prohibición incluye el uso de las computadoras del

Distrito para ayudar o promover, directa o indirectamente, a favor o en contra de una propuesta de votación y/o la elección de cualquier persona a cualquier oficina.

- Uso ilegal o indecente: Está prohibido el uso de la red del Distrito con fines ilegales, de intimidación, acoso, vandalismo, inapropiados o indecentes (incluyendo el acceso, almacenamiento o visualización de material pornográfico, indecente o de otra forma inapropiado), o en apoyo de tales actividades. Las actividades ilegales son cualquier violación de las leyes federales, estatales o locales (por ejemplo, la infracción de derechos de autor, la publicación de información difamatoria, o cometer fraude). El acoso incluye insultos, comentarios, chistes, insinuaciones, cumplidos inoportunos, caricaturas, bromas, o conducta verbal relativa a una persona que (1) tenga el propósito o el efecto o la creación de un entorno intimidatorio, hostil u ofensivo, (2) tenga por objeto o efecto interferir injustificadamente con el trabajo o el rendimiento escolar de una persona, o (3) interfiera con las operaciones escolares. El vandalismo es cualquier intento de dañar o destruir el sistema operativo, software de aplicación, o datos. El uso inapropiado incluye cualquier violación de la finalidad y el objetivo de la red. Las actividades indecentes incluyen violaciones de las normas sociales generalmente aceptadas para el uso de equipos de propiedad y operación pública.

Uso perturbador: la red del Distrito no puede ser utilizada para interferir o interrumpir a otros usuarios, servicios o equipos. Por ejemplo, las interrupciones incluyen la distribución de publicidad no solicitada ("*spam*"), la propagación de virus informáticos, la distribución de grandes cantidades de información que pueden abrumar el sistema (cartas de cadenas, juegos en red o mensajes de difusión), y cualquier acceso no autorizado o la destrucción de las computadoras del Distrito o de otros recursos accesibles a través de la red de computadoras del Distrito ("*cracking*" (piratería) o "*hacking*" (violación de los sistemas)). Esto incluye transferir un programa o ejecutar un programa no autorizado desde una unidad de disco USB en un ordenador.

- Uso personal: La red del Distrito no podrá ser utilizada con fines personales que no estén autorizados específicamente por un maestro u otro integrante del personal del distrito. Esto incluye la conexión de dispositivos personales a la red del distrito.

El distrito no será responsable de los daños y perjuicios sufridos por ningún usuario, incluyendo, pero sin limitarse a, la pérdida de datos como resultado de retrasos, omisiones de entregas, entregas erróneas o interrupciones del servicio causadas por su propia negligencia o por cualquier otro error u omisión. El distrito no será responsable de las obligaciones financieras no autorizadas resultantes de la utilización o el acceso a la red informática del distrito o la Internet.

Seguridad en Internet

Los estudiantes no deben revelar información personal, incluyendo dirección y número de teléfono en los sitios de Internet, correo electrónico, o como contenido en ningún otro medio electrónico. Los estudiantes no deben revelar información personal sobre otra persona en ningún medio electrónico. No se pueden publicar imágenes o nombres de los estudiantes en ninguna clase, escuela, o en el sitio web del distrito a menos que se haya verificado el permiso correspondiente de acuerdo con la política del distrito. Si los estudiantes encuentran información o mensajes peligrosos o inadecuados, deben notificarlo a la autoridad escolar correspondiente.

Instrucción de Seguridad en Internet

A todos los estudiantes se les dará instrucción acerca de la conciencia y la respuesta al ciberacoso y sobre el comportamiento apropiado en línea, incluyendo la interacción con otros individuos en el correo electrónico y/o en los sitios de redes sociales y en las salas de chat. Las escuelas harán todo lo posible para proporcionar instrucciones de seguridad en Internet, sin embargo, en ausencia de tal instrucción, se espera que los estudiantes aún sigan todos los procedimientos de uso aceptable (*AUP*). Materiales apropiados de formación según la edad se pondrán a disposición de la administración, el personal y las familias.

Filtrado y Control

Se utiliza Software de filtrado para bloquear o filtrar el acceso a representaciones visuales que sean obscenas y a toda la pornografía infantil, de conformidad con la Ley de Protección de Niños en Internet (*CIPA*). Otro material censurable podría filtrarse según lo identificado por el superintendente o su designado.

- El software de filtrado no es 100% efectivo. Mientras que los filtros hacen que sea más difícil recibir o visitar material objetable, los filtros no son una solución en sí mismos. Cada usuario debe asumir la responsabilidad por su uso de la red e Internet y evitar sitios de dudosa reputación;
- Está prohibido cualquier intento de anular o sobrepasar el filtro de Internet del distrito u ocultar la actividad de Internet: *proxies*, https, puertos especiales, modificaciones en la configuración del navegador del distrito y cualquier otra técnica diseñada para evadir el filtrado o permitir la publicación de contenidos inapropiados;
- Correo electrónico inconsistente con la misión educativa del distrito será considerado SPAM y se bloqueará la entrada a los buzones de correo electrónico del distrito;
- El distrito proveerá supervisión adecuada de un adulto para el uso de Internet. La primera línea de defensa para controlar el acceso de los menores a material inapropiado en Internet es el control deliberado y consistente del acceso de los estudiantes a las computadoras del distrito;
- Los integrantes del personal que supervisan a los estudiantes, equipos de control electrónico, o que tengan la oportunidad de observar el uso por parte de los estudiantes de dicho equipo en línea deben hacer un esfuerzo razonable para vigilar el uso de este equipo para asegurar que el uso de los estudiantes se ajusta a la misión y los objetivos del distrito, y
- El personal debe hacer un esfuerzo razonable para familiarizarse con la Internet y supervisar, instruir y ayudar eficazmente.

<u>Red de seguridad y privacidad</u>
Las contraseñas son el primer nivel de seguridad de una cuenta de usuario. Los nombres de usuario y las cuentas del sistema sólo se deben utilizar por parte del propietario autorizado de la cuenta, para los propósitos autorizados por el distrito. Los estudiantes son responsables de toda la actividad en su cuenta y no deben compartir su contraseña de la cuenta.

Estos procedimientos están diseñados para proteger las cuentas de usuario de red:

- Cambie las contraseñas de acuerdo con la política del distrito;
- No use la cuenta de otro usuario;
- No utilice dispositivos personales con punto de acceso inalámbricos;
- No conecte los teléfonos inteligentes personales, computadoras personales, dispositivos de almacenamiento personales, o ningún dispositivo que no sea del distrito a las redes del distrito;
- No inserte las contraseñas en el correo electrónico u otras comunicaciones;
- Si escribe su contraseña de la cuenta, manténgala oculta;
- No guarde las contraseñas en un archivo sin cifrar;
- No utilice la opción "recordar contraseña" de los navegadores de Internet, y
- Bloquee la pantalla o cierre la sesión, si deja el equipo.

Datos del estudiante
El personal del distrito debe mantener la confidencialidad de los datos de los estudiantes de acuerdo con la Ley de derechos educativos y privacidad de la familia (*FERPA*). El permiso para publicar cualquier trabajo de los estudiantes requiere el permiso del padre o tutor.

Privacidad
La red del Distrito, las computadoras, la Internet y el uso del correo electrónico no son intrínsecamente seguros o privados. El distrito se reserva el derecho de supervisar, inspeccionar, copiar, revisar y almacenar, sin previo aviso, la información sobre el contenido y la utilización de:

- La red;
- Los archivos de usuario y la utilización de espacio en disco;
- Las aplicaciones de usuario y la utilización del ancho de banda;
- Los archivos de documentos, carpetas y las comunicaciones electrónicas del usuario;
- El correo electrónico;
- El acceso a la Internet y,
- Cualquier y toda la información transmitida o recibida en relación con la red y el uso del correo electrónico.

El distrito se reserva el derecho de revelar cualquier mensaje electrónico a los funcionarios encargados de hacer cumplir la ley o a terceros, según corresponda. Todos los documentos están sujetos a las leyes de divulgación de registros públicos del Estado de Washington. Se hace copia de seguridad de toda la correspondencia de correo electrónico del distrito para fines de divulgación pública y recuperación de desastres.

Derechos de autor
Está generalmente prohibido descargar, copiar, duplicar y distribuir software, música, archivos de sonido, películas, imágenes u otros materiales con derechos de autor sin el permiso expreso y por escrito del propietario del derecho de autor. Sin embargo, la duplicación y la distribución de materiales con fines educativos se permite cuando dicha copia y distribución cae dentro de la ley de uso justo de derechos de autor de los Estados Unidos (Título 17, USC) y el contenido se cita apropiadamente.

Disciplina
La violación de cualquiera de las condiciones de uso explicadas en la póliza del uso de recursos electrónicos por parte del estudiante o en estos procedimientos de uso aceptable (*AUP*) podría ser motivo de acción disciplinaria, hasta e incluyendo la revocación de la red y los privilegios de acceso a la computadora, la restitución, la suspensión o la expulsión y/o informe a la policía, de acuerdo con las políticas y procedimientos de disciplina del Distrito para estudiantes.

Adoptado: 06/25/12

Revisado: 07/10/13

Preguntas frecuentes

¿Qué pasa si un estudiante se olvidó de cargar su computadora portátil y la batería está muerta?
Una de las mejores formas de evitar este problema es recordar consistente (y constantemente) a los estudiantes que carguen el portátil en casa todas las noches. Se espera que traigan el portátil a la escuela cargado todos los días. Si ellos no lo hacen, pueden pedir prestado un cable de alimentación de repuesto. Aparte de eso, el estudiante tendría que cargar su computadora portátil en la ubicación de las computadoras portátiles de la escuela (a menudo la biblioteca) y perder la participación en las actividades del aula con las computadoras portátiles hasta que la batería está cargada.

¿Qué pasa si mi hijo olvidó llevar el portátil a la escuela?
Si un estudiante olvida llevar su portátil a la escuela, el estudiante puede perder la oportunidad de realizar las actividades de instrucción relacionadas con la computadora ese día. Por favor, ¡ayúdenos a que su estudiante traiga su portátil a la escuela todos los días! Cada escuela tiene un número muy pequeño de dispositivos "para préstamo". La prioridad para estos préstamos es para los estudiantes que experimentan problemas de equipos fuera de su control. Cuando estén disponibles, a un estudiante que haya olvidado traer su portátil la escuela le podrá dar un dispositivo de "préstamo".

¿Qué sucede si el portátil de un estudiante se rompe después de la salida?
El estudiante traerá el portátil roto a la escuela para devolverlo. Uno de préstamo/de repuesto se puede prestar en la escuela para minimizar la pérdida de tiempo de instrucción. El estudiante es responsable de la pérdida o daños del portátil de préstamo/de repuesto mientras está en su posesión. Una vez que se repare el portátil original del estudiante, el estudiante recibirá una notificación para cambiar el de préstamo por el portátil original. Si se determina que el daño ha sido causado por negligencia o abuso del estudiante, habrá una multa evaluada por los costos de reparación, como se indica en el contrato.

¿Qué pasa si le roban el portátil?
La pérdida debe ser reportada lo antes posible a la escuela de su estudiante. El estudiante puede entonces retirar uno en préstamo/de repuesto hasta que resolvamos el problema de la pérdida. ¡Es muy importante que el estudiante mantenga una buena seguridad del portátil en todo momento! Por favor trabaje con su hijo para reforzar la importancia de cuidar la computadora portátil.

Mi hijo está en un equipo deportivo y/o tomando Educación Física. ¿Cómo se mantendrá el portátil seguro?
El personal de instrucción de EF y el entrenador indicarán a los estudiantes sobre los procedimientos específicos de esta semana. Un lugar seguro estará disponible para los estudiantes en educación física y en equipos deportivos para mantener las computadoras portátiles seguras durante esos programas.

¿Cómo va a estar mi estudiante protegido de material objetable?
El software de filtración está instalado en cada computadora portátil. Los sitios web objetables son descartados. Sin embargo, ningún sistema de filtrado es perfecto. La seguridad en Internet se le enseña a los estudiantes para ayudarles a mantenerse lejos de materias objetables, así como para

mantenerse seguros en línea. El software de filtrado permanece en el portátil cuando se usa en casa, también.

No permitir que mi estudiante tenga una contraseña en su computadora de la casa para que yo pueda controlar su uso. ¿Cómo puedo saber lo que mi hijo está haciendo en la computadora de la escuela?

Consiga el nombre de usuario y la contraseña con su estudiante. Si bien es cierto que prohibimos compartir contraseñas con usuarios no autorizados, los padres son usuarios explícitamente autorizados. Le animamos a saber lo que su hijo está haciendo en su computadora portátil escolar.

El acceso a Internet en casa es costoso. ¿Las familias están obligadas a proporcionar acceso a Internet en casa?

No, nosotros no requerimos que las familias tengan acceso a Internet, a pesar de que sería muy útil para los estudiantes. Sin embargo, usted debería saber sobre el programa *Comcast Internet Essentials*, que ofrece acceso básico a Internet a las familias con estudiantes que califican para almuerzo gratis o a precio reducido. Este programa ofrece un servicio de Internet en casa por $ 9.95 al mes más impuestos, sin cargos por activación, ni tasas de alquiler de equipos ni aumentos de precios. Para obtener mayor información, visite InternetEssentials.com o llame al 1-855-846-8376.

¿Puede mi estudiante usar su propio computador personal en lugar de un computador brindado por el distrito?

Hay muchas razones por las cuales estamos brindando los mismos dispositivos de cómputo a todos los estudiantes en la escuela. Estas incluyen seguridad, instrucción, apoyo técnico, e igualdad.

Seguridad: hemos instalado filtros web y tenemos otras precauciones de seguridad que ayudan a evitar que los estudiantes accedan a páginas no seguras o inapropiadas mientras estén en la escuela o en la casa. No podemos estar seguros de que los dispositivos traídos de la casa cumplan con los mismos estándares.

Instrucción: hemos comprado e instalado muchos paquetes de software en los portátiles del distrito que no están disponibles en computadores externos. El mismo software, y a veces la misma versión, está en cada portátil del distrito, por lo tanto, los maestros pueden rápida y más eficientemente enseñar a las clases completas y ayudar a los estudiantes de forma individual. Tratar de enseñar una lección con muchos tipos de software y/o versiones diferentes de ese software sería difícil.

Soporte Técnico: podemos brindar apoyo técnico robusto a través de nuestro personal de apoyo técnico a un universo limitado de dispositivos de cómputo. No podemos brindar el mismo nivel de apoyo a un universo ilimitado de dispositivos, ya que esto puede llevar a mayores retrasos con los computadores y pérdidas de oportunidades de aprendizaje. Esta práctica es similar a un sector privado, donde los empleados reciben un dispositivo de propiedad de la compañía para asegurar una experiencia de usuario predecible y apoyo técnico óptimo.

Igualdad: algunas familias no pueden pagar el último computador o incluso ni siquiera un computador. Si todos los estudiantes están usando el mismo dispositivo, ellos pueden enfocarse en lo que están aprendiendo con el dispositivo, no en quién tiene cuál dispositivo y qué más hay en él.

No se prohíbe a los estudiantes que lleven sus dispositivos móviles/computadores a la escuela, sin embargo, los estudiantes que llevan computadores personales:

- También deben llevar su computador del distrito completamente cargado y listo para usar

- Deben usar el dispositivo del distrito cuando un maestro lo solicite
- Puede acceder a internet sólo por medio de la red inalámbrica de invitado, donde hay filtros al nivel de protección necesitado para un estudiante de primaria.
- No recibirá apoyo técnico o apoyo con computadores personales
- Puede no tener acceso a impresión o carga de su computador personal en la escuela
- Haga esto a su propio riesgo. El distrito no se responsabiliza de computadores personales perdidos o robados.

¿Qué ocurre si no firmo el acuerdo? No quiero que mi familia sea responsable del computador portátil. Si ningún padre o tutor firma del acuerdo, el estudiante aún tendrá acceso a un computador cuando él/ella esté en la escuela. Si el estudiante intencionalmente daña el equipo, las familias serán aún responsables de los daños, lo mismo que con cualquier equipo de propiedad de la escuela.

¿Los niños pueden conectarse con la impresora de su casa o tienen que logarlo de una manera diferente?

Para instalar una impresora en casa, siga estos pasos:

1. Haga clic en el botón de Inicio de Windows y escriba **Dispositivos** e **Impresoras** y presione **Ingresar**.
2. Haga clic en "**Agregar una impresora**"
3. Aparece la ventana Agregue Un El dispositivo. Seleccione su impresora y seleccione **Siguiente**
4. Cuando el computador agregue la impresora, haga clic en **Imprimir una Página de Prueba** y/o haga clic en **Finalizar**

Si la impresora no está en la lista de impresoras, puede que tenga que descargar el controlador. Los estudiantes pueden instalar controladores e imprimir en algunas impresoras domésticas.

- Visite el sitio web del fabricante de la impresora y descargue el controlador. Sólo tiene que descargar la versión 'sólo controlador' del software ya que el dispositivo no permitirá la instalación de software de administración de impresión
- Tenga en cuenta la ubicación/carpeta donde se guarda en el controlador
- Por favor tenga en cuenta que las impresoras inalámbricas y de red requieren pasos adicionales y, posiblemente, un software, lo que está más allá del alcance de este documento y que pueden requerir soporte técnico del fabricante. También tenga en cuenta que los estudiantes no pueden instalar software distinto de los controladores en su computador para impresoras que requieran software de administración de impresión ya que pueden no ser compatibles con el dispositivo.

Se prohíbe a los estudiantes la instalación de software por razones de seguridad, lo que también bloqueará la instalación de software de administración de impresión. Consulte con el fabricante para ver si ofrecen la solución de sólo instalar controlador.

¿Cómo llego al dispositivo MAS para agregar la configuración de seguridad de red doméstica personalizada?

Por razones de seguridad, el Distrito no permite a los estudiantes o padres derechos de administración de los dispositivos. Hemos establecido los dispositivos MAS para trabajar con la seguridad común brindada por la mayoría de las redes inalámbricas que se encuentran en empresas, bibliotecas, u hoteles.

Si su seguridad inalámbrica doméstica es más compleja, brindamos las siguientes recomendaciones:

1. Agregue un segmento a su red con menos seguridad para el uso por el dispositivo MAS
2. Conecte el dispositivo MAS directamente a la red doméstica y a la derivación inalámbrica
3. Abra un punto de acceso para el uso por el dispositivo MAS aparte de su red inalámbrica segura
4. Considere el uso de la configuración de seguridad estándar
5. Considere agregar seguridad o filtrado a su dispositivo de red, no al equipo, tal como la que brinda www.opendns.com.

¿Por qué los estudiantes no pueden instalar software en los dispositivos *MAS*?

Estamos obligados por la Ley de Protección de Niños en Internet (*CIPA*) a filtrar el contenido de Internet a cualquier dispositivo al que acceden los estudiantes en la red *LWSD*, incluyendo los dispositivos *MAS*. A algunos estudiantes no les gustan los filtros. Dada la oportunidad, los estudiantes podrían instalar software de seguridad contraproducente para eludir este requisito. Algunos estudiantes también se verían tentados a utilizar los dispositivos para el intercambio ilegal de archivos. Todas esas acciones violan la Política de Uso Aceptable del distrito.

Estoy muy preocupado por lo que mi estudiante puede ver en internet. ¿Qué puedo hacer?

LWSD va más allá de los requisitos legales de *CIPA* e instala en los dispositivos un filtro que funciona en cualquier red. Sin embargo, ningún filtro es 100% confiable. Para proteger aún más a su hijo, le recomendamos que añada filtrado a la red doméstica. Una opción es usar un servicio de filtrado libre como el de www.OpenDNS.com que filtrará el contenido nefasto de su red doméstica en todos los dispositivos, incluyendo el dispositivo *LWSD MAS*. Nuevos sitios web comienzan todos los días y cuando nos damos cuenta de los sitios inapropiados, los bloqueamos. Si el estudiante ha accedido a un sitio web que le causa preocupación y considera que es inapropiado, por favor envíe la dirección URL a webfilter@lwsd.org.

DIGITAL LITERACY AND CITIZENSHIP IN A CONNECTED CULTURE
© 2012 www.commonsense.org 1

Recursos de seguridad en Internet

El distrito ha seleccionado un plan de seguridad en Internet que ha sido desarrollado por *Common Sense Media*. Como parte de este manual, hemos proporcionado algunas de sus hojas de consejos para que los padres puedan apoyar a los estudiantes en el uso de la Internet de forma segura. Se pueden encontrar más recursos en www.commonsense.org

HOJA DE CONSEJOS PARA PADRES ESCUELA INTERMEDIA

Common Sense respecto a la cultura conectada

……..……..

¿Cuál es el problema?

Todos somos parte de las comunidades. Nuestras escuelas, nuestras ciudades, nuestras aficiones o intereses todos forman los centros alrededor de los cuales nos conectamos con otras personas. Todas estas comunidades tienen códigos de conducta (escritos o no) que ayudan a que todos se lleven bien. Pero en el mundo digital de hoy 24/7, también formamos parte de las comunidades en línea. Y estas comunidades nos conectan con gente que tal vez no conozcamos. Nos conectan de manera en la que sólo se nos conoce por el nombre de pantalla, o dónde estamos en el anonimato. Nos conectan con personas que a veces están muy lejos. Ya sea que estemos leyendo o escribiendo una crítica de un restaurante en línea, publicar algo en una página de Facebook, enviar mensajes de texto a un amigo, o compartir una foto en una página web de fotos, estamos participando en un mundo en el que podemos estar conectados al instante con miles de personas en un momento.

¿Por qué es importante?

Cuando nuestros hijos se conectan entre sí ya sea a distancia o por medio de un nombre de pantalla, esto puede afectar la forma en que se comportan. Las acciones pueden estar libres de descubrimiento o consecuencias. Cuando algo sucede anónimamente, es más fácil para las personas comportarse de manera irresponsable, cruel o poco ética. Los chicos se benefician de un código de conducta para la actividad en línea y con móviles de la misma manera que necesitan un código de conducta en el mundo real. Deben ser competentes para ser buenos ciudadanos digitales, además de ser buenos ciudadanos en general. Nuestros hijos están creando comunidades en línea con cada clic del ratón o el texto que envían. Y tendrán que vivir en esas comunidades. La información que publican sobre sí mismos o a los demás va a durar mucho tiempo y va a viajar grandes distancias. Por lo tanto los padres y los maestros deben ayudar a los niños a pensar en las consecuencias de sus acciones en línea. Los niños deben aprender que la manera en la que se comportan cuando están conectados realmente les importa a ellos, a sus amigos y a las comunidades más amplias en las que participan. Por último, hay mucho en juego. Cuando los niños hacen mal uso de la tecnología en línea o de los móviles para acosar, avergonzar, o intimidan a otros, pueden hacer un daño real y duradero.

El sentido común dice:

La cultura conectada puede ser positiva o negativa — es lo que la gente hace. Al guiar a nuestros hijos, es importante que ellos entiendan que tienen una opción en todas sus relaciones en línea. Ellos pueden decir algo positivo o decir algo malo. Pueden crear gran apoyo a la comunidad en torno a actividades o intereses, o pueden abusar de la naturaleza pública de las comunidades en línea para destrozar a los demás.

Hable sobre el ciberacoso: es real. Está en todas partes. Y recuerde que los niños a veces le contarán acerca de los problemas de un amigo en lugar de sus propias experiencias. Asegúrese de que sus hijos sepan cómo hacer frente a un ciberacosador, y que si la situación se agrava, insístales para que le digan a un adulto de confianza al respecto.

Dar a los chicos un vocabulario de acoso cibernético. Hable acerca de matones, víctimas, espectadores (aquellos que son testigos de un comportamiento ofensivo pero no hacen nada para evitarlo), y *upstanders* (personas que activamente tratan de detener el acoso cibernético). Esto les ayudará a entender qué papel juegan o podrían jugar.

Anímelos a hacer publicaciones positivas. ¿Son sus hijos fanáticos de *YouTube*? ¿Han dicho algo alentador acerca de algo que han visto y les ha encantado? ¿Han añadido conocimientos a un wiki o compartido su experiencia en un sitio de aficiones o intereses? Desde los primeros años, los niños necesitan saber que pueden hacer publicaciones positivas al mundo en línea.
Recuerde a los niños que los textos y mensajes instantáneos pueden no persistir, pero aún así tienen impacto. Todo lo que dicen o hacen con sus teléfonos o a través de mensajes instantáneos parecen desaparecer cuando los dispositivos se apagan, pero el impacto en los demás permanece — ya sea para bien o para mal.

HOJA DE CONSEJOS PARA PADRES ESCUELA INTERMEDIA Y SECUNDARIA

Common Sense respecto al acoso cibernético

¿Cuál es el problema?

El ciberacoso es el uso de herramientas de medios digitales, tales como Internet y los teléfonos celulares, para humillar deliberadamente y acosar a otros, muchas veces de manera repetida. Aunque la mayoría de los adolescentes no hacen esto, los que lo hacen son a menudo motivados por un deseo de poder, estatus, y atención - y sus objetivos son a menudo las personas que están compitiendo por la posición social. Los acosadores cibernéticos a menudo se aprovechan del anonimato de la Web para antagonizar a alguien sin ser reconocido.

El ciberacoso puede tomar una variedad de formas, tales como acosar a alguien, hacerse pasar por alguien, difundir rumores, o reenviar información embarazosa sobre una persona. Los comentarios mezquinos de un acosador pueden propagarse ampliamente a través de la mensajería instantánea (*IM*), los mensajes de texto del teléfono y por mensajes en sitios de redes sociales. Esto puede suceder rápidamente, con poco tiempo para que los adolescentes se tranquilicen entre las respuestas. Y puede suceder en cualquier momento -en la escuela o en el hogar- y muchas veces involucra grandes grupos de adolescentes.

¿Por qué es importante?

El ciberacoso es similar al acoso cara a cara, pero las herramientas en línea magnifican el dolor, la humillación y el drama social de manera muy pública. Ya se trate de la creación de una página falsa de *Facebook* o *MySpace* para hacerse pasar por un compañero de estudios, el envío de mensajes de texto e imágenes en varias ocasiones hirientes, o la difusión de rumores o publicar comentarios crueles en Internet, el acoso cibernético puede resultar en daño emocional e incluso físico severo.

Y aunque cualquiera puede observar el comportamiento de ciberacoso en el mundo real, es mucho más difícil de detectarlo en el mundo en línea. A veces, todo un círculo social se involucrará, y luego se vuelve más difícil para un adolescente individual retirarse de este. De hecho, grupos enteros de adolescentes pueden estar participando de forma activa o pasiva, y el objetivo puede sentir que es imposible escapar de los acosadores. Además, la información que hace daño publicada en Internet es extremadamente difícil de quitar, y millones de personas pueden verla.

Los siguientes consejos pueden ayudarle a reconocer las señales de advertencia de ciberacoso y servir como una guía para hablar con sus hijos adolescentes sobre la prevención del mismo.

Lo que las familias pueden hacer

Pareces triste. ¿Qué está pasando en la escuela? ¿Hay algo inquietante que está sucediendo en línea?

Estoy aquí para tí y también lo están tus amigos. Habla conmigo en cualquier momento.

¿Hay maestros en la escuela que hayan tratado con este tipo de situaciones antes? Creo que deberías decirle a uno de ellos acerca de lo que está ocurriendo.

Los acosadores quieren atención, poder y estatus, lo que explica por qué tienen que hacer drama.

Vi una noticia sobre un adolescente que fue acosado en línea. ¿Qué harías tú en esa situación?

El sentido común dice:

Reconozca el contexto. El Ciberacoso con frecuencia no se considera como "ciberacoso" para los adolescentes involucrados. A pesar de que un incidente tiene una historia, argumento, y matices, en lugar de referirse a "ciberacoso", intente con las palabras "crueldad digital", "abuso" o "ser malo" en línea.

Ayude a los adolescentes a entender cuando el comportamiento cruza la línea. Ayude a su adolescente a sintonizarse con sus propios sentimientos. Si se sienten miedo emocional o físicamente, es el momento de buscar ayuda.

Fomente la empatía. Los adolescentes comprenden el impacto perjudicial del ciberacoso en las personas que se dirige este, ahora y en el futuro. Anímelos a escuchar a las víctimas y a convertirse en sus aliados.

Sea realista. Los adolescentes tienen sus propias dinámicas sociales que a menudo no incluyen a los padres, por lo que ayudarles directamente puede ser difícil. Anime a los adolescentes a encontrar amigos u otros adultos de confianza para ayudarles a superar la situación, incluso si no es usted. Los sitios web con frecuencia son lentos para responder, si es que responden, pero reportar un incidente a un administrador del sitio web puede ser un paso importante.

Recuerde que su hijo podría ser el acosador. Los adolescentes pueden tener diferentes roles en el acoso cibernético en diferentes momentos. Un adolescente que es acosado cibernéticamente podría cambiar su papel y acosar cibernéticamente a alguien más para sentirse poderoso nuevo. Haga preguntas para entender qué papel o papeles están jugando sus hijos adolescentes.

Dígales que se desvinculen. Anime a sus hijos adolescentes a ignorar y bloquear al acosador, e incluso cerrar la sesión en el equipo por un tiempo. Señale que los acosadores cibernéticos con frecuencia están sólo buscando atención y posición, así que no se les debe permitir que sus esfuerzos han dado resultado.

HOJA DE CONSEJOS PARA PADRES ESCUELA INTERMEDIA

Common Sense respecto a hablar en línea de manera segura

¿Cuál es el problema?

A los chicos les encanta conectarse con otras personas en línea. La mayoría de los jóvenes hablan en línea con sus amigos y familiares en lugar de con extraños. Pero como padre, usted podría estar preocupado de que un desconocido con malas intenciones pueda ponerse en contacto con su hijo.

"El comportamiento depredador en línea," como se le conoce comúnmente, es cuando los adultos contactan niños o adolescentes a través de Internet en un intento de "preparar a los niños utilizando habilidades manipuladoras" (*groom*) para tener relaciones sexuales inapropiadas. Muchos expertos, sin embargo, han encontrado que la amenaza más realista para los adolescentes en línea es en realidad la "solicitud sexual en línea." Esto significa animar a alguien para hablar de sexo, dar información sexual personal, o enviar fotos sexuales o de vídeo. (No siempre significa pedir sexo.) Por ejemplo, los adolescentes podrían recibir solicitudes inapropiadas o mensajes de desconocidos o conocidos. Sin embargo, contrariamente a la creencia popular:

- Los adolescentes (edades 13-17) están en mayor riesgo de recibir solicitudes en línea que los "preadolescentes" o niños
- La mayoría de las solicitudes en línea provienen de los mismos adolescentes, o de adultos jóvenes (entre 18 y 25)
- Los adultos que hacen solicitudes a los adolescentes suelen ser directos acerca de su verdadera edad y sus intenciones (Subrahmanyam y Smahel, 2011).

¿Por qué es importante?

Cuando los adolescentes son conducidos por mal camino respecto a lo que deben buscar en línea, pueden encontrarse en situaciones peligrosas sin darse cuenta. El encanto de este tipo de relaciones no es sorprendente, sobre todo para los adolescentes que ya son vulnerables. Los que hacen las solicitudes pueden proporcionar a los adolescentes un aumento en la autoestima con elogios y atención. Y una vez que los adolescentes se involucran en estas relaciones, podrían estar de acuerdo en hacer cosas que normalmente no harían debido al desequilibrio de poder entre ellos y el que hace la solicitud. Con frecuencia no es hasta mucho después que se dan cuenta de que estaban siendo manipulados.

El sentido común dice:

Hable acerca del comportamiento responsable en línea. Hable acerca de con quién está bien hablar y acerca de qué está bien hablar. Recuerde que muchos adolescentes están empezando a experimentar con el coqueteo y las relaciones. Esto es normal. Pero coquetear en línea con extraños o conocidos es siempre arriesgado. El coqueteo puede conducir rápidamente a conversaciones o peticiones inapropiadas. También puede llevar a los adolescentes jóvenes a creer que están en una relación seria, romántica con alguien que en realidad no conocen. Ambas situaciones pueden hacer que los adolescentes se sientan incómodos o manipulados.

Bloquear, ignorar o salir. La mayoría de los adolescentes saben cómo no hacer caso a un contacto no deseado. Anime este comportamiento.

Asegúrese de que su hijo se siente seguro para hablar con un adulto de confianza. Si pasa algo espeluznante o inapropiado, los adolescentes jóvenes necesitan saber que no se van a meter en problemas si le cuentan a usted u otro adulto de confianza sobre esto.

Hable con su hijo acerca de relaciones saludables. Puede ser difícil para algunos jóvenes adolescentes reconocer cuando otras personas los están manipulando, especialmente aquellos jóvenes adolescentes que quieren experimentar

o probar que son maduros. Discuta qué factores hacen relaciones saludables, y por qué los adolescentes no deben comprometer estos valores.

Busque señales de advertencia. ¿Su hijo parece introvertido, que pasa horas interminables en línea, o parece estar escondiendo algo? Los adolescentes jóvenes que terminan en relaciones en línea inapropiadas con frecuencia muestran estas señales de advertencia. Si usted piensa que esto podría estar ocurriendo, pregúntele a su hijo al respecto.

Fuentes

The Berkman Center for Internet & Society en *Harvard University*. Enhancing Child Safety & Online Technologies: Final Report of the Internet Safety Technical Task Force. 2008. (Mejorando la Seguridad de los Niños y las tecnologías en línea: Informe Final del Grupo de Trabajo Técnico de Seguridad en Internet. 2008).

Smith, A. "*Teens and Online Stranger Contact*." (Adolescentes y contacto extraño en línea). *Pew Internet & American Life Project*. Oct 14, 2007. (http://www.pewinternet.org/Reports/2007/A.aspx).

Subrahmanyam, K., and Smahel, D. *Digital Youth: The Role of Media in Development*. (Juventud Digital: El papel de los Medios de Comunicación en el Desarrollo), 2011, Springer, New York.

Ybarra, M., and Mitchell, K. J. "*How Risky Are Social Networking Sites? A Comparison of Places Online Where Youth Sexual Solicitation and Harassement Occurs*." (¿Qué tan riesgoso son los sitios de redes sociales? Una comparación de lugares en línea donde ocurren el acoso y las solicitudes sexuales) *Pediatrics* (2008). 121(2), pp. e350-e357.

Wolak, K., Mitchell, K., and Finkelhor, D. "*Online Victimization of Youth: Five Years Later*." (Victimización en línea de la Juventud: Cinco años después). 2006. *National Center for Missing & Exploited Children Bulletin*. (http://www.unh.edu/ccrc/pdf/CV138.pdf).