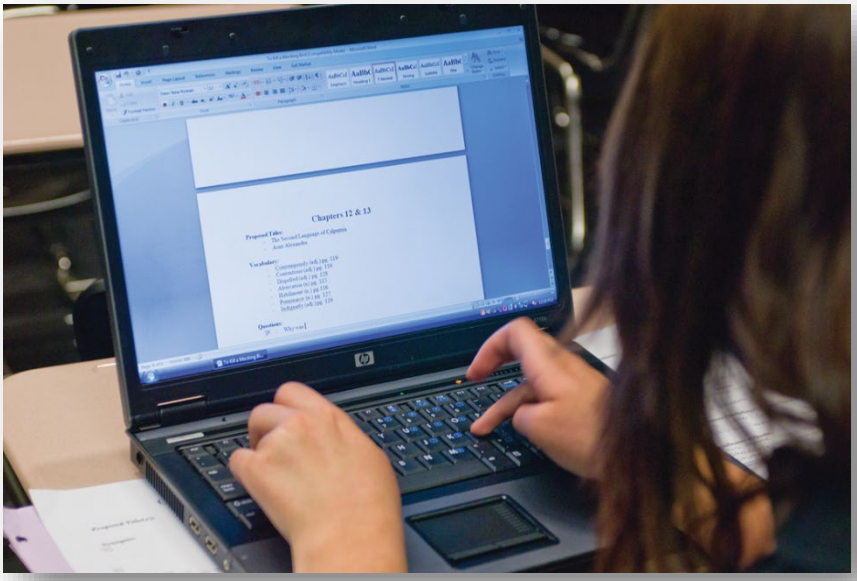

Manual del Portátil

Contenido

Generalidades

El programa de Acceso Móvil para Estudiantes proporciona a cada estudiante del Distrito Escolar de Lake Washington un computador portátil para su uso educativo. El uso de esta herramienta está diseñado para enriquecer el ambiente de aprendizaje y para ayudar a los maestros mientras apoyan a los estudiantes en la adquisición de las habilidades, conocimientos y atributos descritos en el Perfil del Estudiante del distrito.

El acceso a la red escolar y a los recursos informáticos es una oportunidad para aprender la responsabilidad del uso informado, ético y responsable de los computadores. Este manual describe muchas de estas responsabilidades y brinda información y recursos para las familias sobre estas expectativas.

Responsabilidades del Padre/Tutor

- Revisar los reglamentos y lineamientos del portátil
- Revisar los *Procedimientos de Uso Aceptable del Estudiante*
- Monitorear el uso del dispositivo del estudiante cuando no esté en la escuela
- Asegurar que el portátil tenga un cuidado adecuado cuando el estudiante en esté en la escuela

Reglamentos & Lineamientos de Uso del Portátil

hela siguiente información se resume del Procedimiento de Uso Aceptable del Estudiante del distrito. Por favor revise la sección del Uso del Estudiante de los Recursos Electrónicos sobre las Políticas y Reglamentos en el sitio web del distrito. Los estudiantes deben entender y seguir estos procedimientos.

- Lo que se debe hacer:
  - Usar el equipo con propósitos educativos.
  - Usar el equipo de forma apropiada.
  - Usar el buen juicio.
  - Proteger las claves:
    - Cambie la clave según sea necesario cada 90 días después del inicio de las clases.
    - No comparta su contraseña ni utilice la cuenta de otra persona.
    - No ponga su contraseña en un correo electrónico u otro mensaje.
    - Si la escribe, guárdela en un lugar seguro.
    - No utilice la función "recordar contraseña" del navegador.
    - Bloquee la pantalla o cierre la sesión si usted se aleja del portátil.
- Lo que no se debe hacer:
  - No utilice el equipo con fines comerciales o en beneficio propio.
  - No utilice el equipo con fines políticos, como intentar influir en las elecciones.
  - No utilice el equipo para nada ilegal o indecente. No se debe realizar ninguna actividad ilegal, intimidar, acosar o mostrar imágenes inapropiadas.
  - No utilice el equipo de forma que perjudique a otros usuarios, servicios o equipos; no haga spam o virus, ni cargue grandes cantidades de datos o intente piratear o crackear sistemas.
  - No intente eludir el filtrado, utilizar proxies, puertos especiales o cambiar la configuración del navegador.
  - No instale, desinstale o modifique ninguna aplicación, juego o componente del sistema operativo.
  - No descargue emuladores de juegos, clientes de chat o software peer to peer.
  - No coloque adhesivos ni marque de ninguna manera el portátil. Los adhesivos dejan residuos en las partes del portátil que son difíciles de eliminar. Usted puede utilizar adhesivos extraíbles.
- Seguridad en Internet:
  - Nunca revele información personal sobre usted u otra persona.
  - No publique fotos o nombres de estudiantes en ningún sitio web sin el permiso de la escuela.
  - Si usted ve algo peligroso o inapropiado infórmele a un maestro inmediatamente.

- Sigua las instrucciones de la escuela sobre la seguridad en Internet, el acoso cibernético y el buen comportamiento en línea.

- **Filtrado, Monitoreo & Seguridad en la Red:**
  - El distrito utiliza un software de filtrado destinado a bloquear el material inapropiado o censurable. El software de filtrado no siempre detecta el material inapropiado. Cada usuario es responsable de evitar los sitios inapropiados.
- **Información & Privacidad del Estudiante:**
  - El personal mantiene la confidencialidad de los datos de los estudiantes de acuerdo con la ley federal (FERPA). Se necesita el permiso de los padres o tutores para publicar el trabajo de los estudiantes.
  - El uso de la red del distrito, las computadoras, el internet y el correo electrónico no son inherentemente seguros o privados. El distrito se reserva el derecho de monitorear, revisar y almacenar y/o revelar cualquier mensaje electrónico a los oficiales de la ley o a terceros.
  - Los documentos, incluido el correo electrónico, están sujetos a las leyes de divulgación de registros públicos. Se hace una copia de seguridad de toda la correspondencia de correo electrónico del distrito para su divulgación pública y recuperación en caso de desastre.
- **Derechos de Autor:**
  - No guarde ni copie ningún material protegido por derechos de autor sin el permiso del propietario, a menos que cumpla con la Doctrina de Uso Justo de la Ley de Derechos de Autor de los Estados Unidos.
- **Infracciones de los Procedimientos de Uso Aceptable del Estudiante:**
  - Se aplican las normas de conducta de la escuela y el uso inadecuado puede dar lugar a medidas disciplinarias. Usted podría ser denunciado a la policía si participa en una actividad ilegal. Consulte las Políticas y Procedimientos de Disciplina Estudiantil del Distrito para obtener más información.

Uso & Cuidado del Portátil

- Traiga el dispositivo a la escuela, completamente cargado, cada día a menos que se le indique lo contrario.
- Permita siempre que el escaneo o la actualización de un equipo complete su proceso.
- Asegúrese de que el equipo no se pierda, sea robado o se dañe, llevando un registro y cuidando el equipo:
  - No deje el equipo sin vigilancia y siga las reglas de la escuela para asegurar, cuando sea necesario, por ejemplo, durante las actividades deportivas.
  - No fuerce la apertura de la tapa del ordenador más allá de su punto de parada.
  - No raye ni estropee el exterior del dispositivo.
  - No quite el código de barras de identificación del distrito.

- No introduzca objetos extraños (clips, bolígrafos) en el dispositivo.
- No coma ni beba cerca del dispositivo móvil.
- Utilice el equipo en una superficie plana y estable.
- En el salón, la tapa del dispositivo debe estar cerrada entre usos.
- Cuando el equipo no esté en uso, debe estar apagado.
- Asegúrese de REINICIAR el equipo de forma regular.
- Utilice únicamente métodos de limpieza adecuados:
- No utilice agua ni soluciones de limpieza.
- Limpie ligeramente las superficies con un paño limpio y suave o con toallitas para el monitor.

Consecuencia por el uso inapropiado, la pérdida o el año del portátil

- El uso inadecuado o el comportamiento en conflicto con las reglas de la escuela tendrá consecuencias de acuerdo con las políticas de disciplina de la escuela y puede incluir:
  - Medidas correctivas, incluyendo un acceso más restrictivo a los recursos informáticos
  - Suspensión/expulsión por infracciones graves o repetidas.
- Si el equipo se pierde o es robado
  - Informar inmediatamente a la escuela de los dispositivos perdidos.
  - Si el dispositivo es robado, se debe presentar una denuncia a la policía y entregar una copia a la escuela.

Acceso a Internet

¿Necesita un servicio de Internet doméstico asequible? El acceso a Internet se ha convertido en algo fundamental para que los estudiantes aprendan en casa y para que las familias se comuniquen con la escuela.

Usted puede encontrar información en la página web del Distrito para Computadoras/Acceso a Internet: Recursos Comunitarios - Distrito Escolar de Lake Washington (lwsd.org) y la nueva página federal Get Internet: Get Internet | La Casa Blanca

El distrito ofrece puntos de acceso celular gratuitos a las familias que lo necesiten. Póngase en contacto con su escuela directamente para obtener más información sobre cómo comprobarlos.

Política & Procedimientos de Uso del Estudiante de los Recursos Electrónicos

Alcance

Los siguientes procedimientos aplican a todos los estudiantes del Distrito y cubren todos los aspectos de la red del Distrito. La red del distrito incluye computadoras/dispositivos alámbricos e inalámbricos y equipo periférico, archivos y almacenamiento, correo electrónico y contenido de Internet y todo el software, las aplicaciones o los recursos informáticos con licencia del Distrito.

Uso Apropiado de la Red

El Distrito espera que los estudiantes tengan buen criterio al utilizar el equipo informático de manera apropiada. Se espera que el uso del equipo esté relacionado con propósitos educativos.

Si el equipo personal se utiliza en las redes del distrito, el distrito se reserva el derecho de acceder al dispositivo para analizarlo y resolver cualquier problema o amenaza identificada. Como condición para el uso de las redes del distrito, el estudiante deberá brindar inmediatamente el dispositivo solicitado.

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

- Uso comercial: Se prohíbe el uso de la red del distrito para beneficio personal o privado, negocios personales o ventajas comerciales.
- Uso Político: Se prohíbe el uso de la red del Distrito para fines políticos en infracción de las leyes federales, estatales o locales. Esta prohibición incluye el uso de las computadoras del Distrito para ayudar o abogar, directa o indirectamente, a favor o en contra de una propuesta electoral y/o la elección de cualquier persona para cualquier cargo.
- Uso ilegal o indecente: Se prohíbe el uso de la red del Distrito para propósitos ilegales, de intimidación, acoso, vandalismo, inapropiados o indecentes (incluyendo el acceso, almacenamiento o visualización de material pornográfico, indecente o inapropiado), o en apoyo de tales actividades. Las actividades ilegales son cualquier infracción de las leyes federales, estatales o locales (por ejemplo, la infracción de los derechos de autor, la publicación de información difamatoria o la comisión de fraude). El acoso incluye calumnias, comentarios, bromas, insinuaciones, cumplidos no deseados, caricaturas, bromas o conducta verbal relacionada con un individuo que (1) tenga el propósito o el efecto de crear un ambiente intimidante, hostil u ofensivo; (2) tenga el propósito o el efecto de interferir irrazonablemente con el trabajo o el rendimiento escolar de un individuo, o (3) interfiera con las operaciones escolares. El vandalismo es cualquier intento de dañar o destruir el sistema operativo, el software de aplicación o los datos. El uso inapropiado incluye cualquier infracción del propósito y objetivo de la red. Las actividades indecentes incluyen la infracción 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 usada 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 puedan sobrecargar el sistema (cartas en cadena, juegos en red o difusión de mensajes) y cualquier acceso no autorizado o destrucción de los computadores del Distrito u otros recursos accesibles a través de la red informática del Distrito ("Cracking" o "Hacking").
- Uso personal: La red del distrito no puede ser utilizada para propósitos de uso personal que no estén específicamente autorizados por un maestro u otro miembro del personal del distrito. Esto incluye la conexión de dispositivos personales a la red del distrito.

El distrito no será responsable de los daños sufridos por cualquier usuario, incluyendo, pero sin limitarse a, la pérdida de datos resultante de los retrasos, la falta de entrega, las entregas perdidas, o las interrupciones del servicio causadas por su propia negligencia o cualquier otro error u omisión. El

distrito no será responsable de las obligaciones financieras no autorizadas que resulten del uso o del acceso a la red informática del distrito o a Internet.

Seguridad en Internet
Los estudiantes no deben revelar información personal, incluyendo la dirección de casa y el número de teléfono en sitios web, correo electrónico, o como contenido en cualquier otro medio electrónico. Los estudiantes no deben revelar información personal sobre otro individuo en ningún medio electrónico. No se pueden publicar fotos o nombres de estudiantes en ningún sitio web de la clase, la escuela o el 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 inapropiados, deben notificar a la autoridad escolar correspondiente.

Instrucción sobre la seguridad en Internet
Todos los estudiantes recibirán entrenamiento sobre la concienciación y la respuesta al acoso cibernético 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 brindar instrucción de seguridad en Internet; sin embargo, en ausencia de dicha instrucción, se espera que los estudiantes sigan los Procedimientos de Uso Aceptable (AUP). Se pondrán a disposición de la administración, el personal y las familias materiales de formación adecuados a la edad.

Filtrado y supervisión
El software de filtrado se utiliza para bloquear o filtrar el acceso a las representaciones visuales que son obscenas y a toda la pornografía infantil de acuerdo con la Ley de Protección de los Niños en Internet (CIPA). Otro material objetable podría ser filtrado según lo identificado por el superintendente o su designado.

- El software de filtrado no es 100% efectivo. Aunque los filtros dificultan la recepción o el acceso a material censurable, no son una solución en sí mismos. Cada usuario debe asumir la responsabilidad de su uso de la red y de Internet y evitar los sitios censurables, lo que incluye abandonar inmediatamente los sitios inapropiados e informar a los funcionarios de la escuela.
- Se prohíbe cualquier intento de anular o eludir el filtro de Internet del distrito o de ocultar la actividad en Internet: proxies, https, puertos especiales, modificaciones de la configuración del navegador del distrito, uso de dispositivos Wi-Fi portátiles personales y cualquier otra técnica diseñada para eludir el filtro o permitir la publicación de contenidos inapropiados.
- Está estrictamente prohibido el uso de emuladores USB (también conocidos como "thumb drive") para ejecutar juegos, eludir el proxy o ejecutar de otro modo archivos .exe no instalados por el distrito u otro software de emulación. Las unidades USB sólo deben utilizarse para contenidos no ejecutables y relacionados con la escuela.
- El almacenamiento brindado por el distrito (por ejemplo, OneDrive, Outlook, el disco duro del portátil o el cuaderno de clase) es para almacenar sólo el contenido generado como parte de la educación del estudiante o requerido para el proceso educativo. Está estrictamente prohibido el intento de almacenar o el almacenamiento de juegos o cualquier archivo ejecutable o contenido inapropiado.
- El correo electrónico inconsistente con la misión educativa del distrito será considerado SPAM y se bloqueará su entrada en los buzones de correo electrónico del distrito.

- El distrito brindará una supervisión adulta apropiada del uso de Internet. La primera línea de defensa para controlar el acceso de los menores a material inapropiado en Internet es la supervisión deliberada y constante del acceso de los estudiantes a los ordenadores del distrito.
- Los miembros del personal que supervisan a los estudiantes, controlan los equipos electrónicos o tienen ocasión de observar el uso de dichos equipos en línea por parte de los estudiantes, deben hacer un esfuerzo razonable para supervisar el uso de estos equipos con el fin de garantizar que el uso por parte de los estudiantes se ajuste a la misión y los objetivos del distrito; y
- El personal debe hacer un esfuerzo razonable para familiarizarse con Internet y para supervisar, instruir y ayudar de manera efectiva.

Seguridad y Privacidad de la Red

Las contraseñas son el primer nivel de seguridad de 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 los fines autorizados del distrito. Los estudiantes son responsables de toda la actividad de su cuenta y no deben compartir su contraseña.

Estos procedimientos están diseñados para salvaguardar las cuentas de los usuarios de la red:

- Cambie las contraseñas de acuerdo con la política del distrito.
- No utilice la cuenta de otra persona.
- No utilice dispositivos inalámbricos personales mientras usted esté en la escuela.
- No conecte teléfonos inteligentes personales, computadoras personales, dispositivos de almacenamiento personales o cualquier dispositivo que no sea del distrito a la red LAN o WLAN del distrito. Se permite la conexión a la red GUEST.
- No inserte contraseñas en el correo electrónico u otras comunicaciones.
- Si usted escribe la contraseña de su cuenta, guárdela fuera de la vista.
- No almacene las contraseñas en un archivo sin cifrar.
- No utilice la función "recordar contraseña" de los navegadores de Internet.
- Bloquee la pantalla o cierre la sesión si usted se aleja del computador.

Los intentos de instalación o la instalación de programa maligno, software de derivación de proxy, red, herramientas de administración, herramientas de administración local o cualquier software, programa maligno o herramienta que permita la manipulación de cuentas de usuario o privilegios administrativos están estrictamente prohibidos. Dichos intentos de instalación o la instalación de dicho programa maligno, software o herramientas se considerarán una falta de conducta excepcional.

Datos de los estudiantes

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). La publicación de cualquier trabajo del estudiante requiere el permiso de los padres o tutores.

Privacidad

La red del Distrito, los computadores, Internet y el uso del correo electrónico no son inherentemente seguros o privados. El distrito se reserva el derecho de supervisar, inspeccionar, copiar, revisar y almacenar, sin previo aviso, información sobre el contenido y el uso de:

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

Derechos de Autor

Por lo general, está prohibido descargar, copiar, duplicar y distribuir software, música, archivos de sonido, películas, imágenes u otros materiales con derechos de autor sin el permiso específico por escrito del propietario de los derechos. Sin embargo, la duplicación y distribución de materiales con fines educativos está permitida cuando dicha duplicación y distribución se ajusta a la Doctrina de Uso Justo de la Ley de Derechos de Autor de los Estados Unidos (Título 17, USC) y el contenido se cita adecuadamente.

Disciplina

La infracción de cualquiera de las condiciones de uso explicadas en la política de Uso de Recursos Electrónicos por parte de los Estudiantes o en estos Procedimientos de Uso Aceptable (AUP) podría ser causa de acción disciplinaria, hasta e incluyendo la revocación de los privilegios de acceso a la red y a las computadoras, restitución, suspensión o expulsión, y/o reporte policial de acuerdo con las Políticas y Procedimientos de Disciplina Estudiantil del Distrito.

Adoptado:
06/25/2012

Modificado:
07/10/2013
10/16/2017
7/2/2018
7/23/2019
8/5/2020
7/2/2021
5/18/2022

Preguntas Frecuentes

¿Qué pasa si un estudiante se olvida de cargar su portátil y se queda sin batería?
Una de las mejores maneras de evitar este problema es recordar constantemente a los estudiantes que carguen el portátil en casa todas las noches. Se espera que traigan el portátil cargado a la escuela todos los días. Si no lo hacen, ellos pueden solicitar un portátil de préstamo en la biblioteca para ese día. De no ser así, el estudiante tendrá que cargar su portátil en el lugar de la escuela donde se encuentra el portátil (a menudo la biblioteca) y perderá la participación en las actividades del salón con el portátil hasta que la batería esté cargada.

¿Qué ocurre si mi estudiante se ha olvidado de traer el portátil al colegio?
Si un estudiante se olvida de traer su portátil a la escuela, puede perderse las actividades de enseñanza relacionadas con el portátil ese día. Por favor, ayude a su estudiante a traer su portátil a/desde la escuela diariamente. Cada escuela dispone de un número muy reducido de dispositivos de "préstamo". La prioridad para estos préstamos es para los estudiantes que experimentan problemas con el equipo que están fuera de su control. Cuando el portátil esté disponible, un estudiante que haya olvidado su portátil puede recibir un dispositivo de "préstamo" de la escuela.

¿Qué sucede si el portátil de un estudiante se daña después de la salida?
El estudiante deberá traer el portátil dañado a la escuela para entregarlo. Un préstamo/repuesto puede obtenerse en el momento para minimizar la pérdida de tiempo de instrucción. Una vez que el portátil original del estudiante esté reparado, se le notificará para que cambie el préstamo por el portátil original.

¿Qué pasa si me roban el portátil?
El robo debe ser informado lo antes posible a la escuela de su estudiante junto con un informe policial. El estudiante puede obtener un préstamo/recambio hasta que se resuelva el problema del robo. Es fundamental que el estudiante mantenga siempre una buena seguridad para el portátil. Por favor, trabaje con su estudiante para reforzar la importancia de cuidar el portátil.

Mi estudiante está en un equipo deportivo y/o está tomando educación física. ¿Cómo puede mantener seguro el portátil?
El personal de educación física y los entrenadores instruirán a los estudiantes sobre los procedimientos específicos. Se pondrá a disposición de los estudiantes de educación física y de los equipos deportivos un lugar seguro para mantener los portátiles durante esos programas.

¿Cómo se mantiene la seguridad de los estudiantes en línea?
Cuando los estudiantes usan los portátiles emitidos por el distrito, mientras están en la escuela o en casa, acceden a Internet a través de los sistemas de filtrado y seguridad del distrito. Estos sistemas se brindan para ayudar a garantizar la seguridad en línea de los estudiantes mientras exploran la Red. También están diseñados para cumplir con los requisitos federales descritos en la Ley de Protección de los Niños en Internet (CIPA) con la que el distrito debe cumplir. El filtrado informático de LWSD se basa en sistemas de seguridad y en Microsoft. Estos sistemas de filtrado de última generación se utilizan para bloquear el material inapropiado u objetable y brindar entornos informáticos en línea para los estudiantes que apoyan su educación. Sin embargo, ningún sistema de filtrado es 100% seguro. Se ha informado de que cada día se crean más de 33.000 sitios web y es posible que se pasen por

alto nuevos sitios con material objetable para los estudiantes o que aún no hayan sido indexados para su filtrado. Los estudiantes son responsables de ayudar a garantizar su seguridad en línea y deben informar de cualquier sitio inapropiado, así como abandonar inmediatamente el sitio. La Política de Uso Aceptable del distrito prohíbe el uso de proxy bypass u otras herramientas que puedan eludir los sistemas de filtrado del distrito.

Las categorías generales de los sitios bloqueados por los cortafuegos de los distritos incluyen: Alcohol, tabaco y drogas; desnudez y contenido para adultos; citas; redes sociales; juegos, shareware y freeware; streaming de medios y compra y descarga de música; alojamiento web y correo electrónico basado en la web, almacenamiento y copia de seguridad en línea; hacking, malware y phishing; portales de Internet, sitios personales y blogs, direcciones IP privadas; derivación/evitación de proxy y DNS dinámico; y sitios de traducción que pueden eludir los sistemas de filtrado; así como otros contenidos objetables identificados.

El personal tecnológico del distrito puede bloquear otros sitios identificados como de contenido inapropiado. Si los sitios dentro de las categorías bloqueadas son necesarios para fines educativos específicos, los maestros pueden solicitar que se abran esos sitios para su acceso.

Los estudiantes que utilizan los computadores del distrito fuera de la escuela tienen un túnel de vuelta a través de los cortafuegos del distrito para que no puedan eludir los filtros de seguridad para estudiantes mientras están conectados a redes privadas.

No permito que mi estudiante tenga una contraseña en su computador en la casa para poder controlar su uso. ¿Cómo puedo saber lo que hace mi estudiante en el portátil de la escuela?
Solicite a su estudiante el nombre de usuario y la contraseña. Aunque prohibimos compartir las contraseñas con usuarios no autorizados, los padres son usuarios autorizados explícitamente. Le animamos a que sepa lo que hace su estudiante en su portátil de la escuela.

El acceso a Internet en casa es costoso. ¿Las familias están obligadas a brindar acceso a Internet en casa?
No, no exigimos a las familias que tengan acceso a Internet, aunque sería muy útil para los estudiantes. Sin embargo, usted debería conocer el programa Comcast Internet Essentials, que brinda acceso básico a Internet a las familias con estudiantes que cumplen los requisitos para recibir un almuerzo gratuito o a precio reducido. Este programa ofrece servicio de Internet en casa por un precio mensual reducido. Para más información, visite InternetEssentials.com o llame al 1-855-846-8376. Se puede encontrar información en la página web del Distrito para Computadoras/Acceso a Internet: Recursos Comunitarios - Distrito Escolar de Lake Washington (lwsd.org) y la nueva página federal Get Internet: Get Internet | La Casa Blanca
El distrito ofrece puntos de acceso celular gratuitos a las familias que lo necesiten. Póngase en contacto directamente con su escuela para obtener más información sobre cómo comprobarlos.

¿Puede mi estudiante utilizar su propio portátil en lugar de uno brindado por el distrito?
Hay varias razones por las que brindamos los mismos dispositivos informáticos a todos los estudiantes en la escuela. Entre ellas están la seguridad, la instrucción, el apoyo técnico y la igualdad.

Seguridad: hemos instalado filtros web y tenemos otras precauciones de seguridad que ayudan a evitar que los estudiantes accedan a sitios web inapropiados o inseguros mientras están en la escuela o en casa. No podemos asegurar que los dispositivos traídos de la casa cumplan la misma norma.

Instrucción: hemos comprado e instalado varios paquetes de software diferentes en los portátiles del distrito que no estarán disponibles en los portátiles externos. El mismo software, e incluso la misma versión, estará en cada portátil del distrito, de modo que los maestros puedan enseñar de forma rápida y más eficiente a clases enteras y ayudar a estudiantes individuales. Intentar impartir una clase con varios tipos de software y/o diferentes versiones de ese software sería muy difícil.

Soporte técnico: LWSD brinda soporte técnico robusto a través de nuestro equipo de soporte técnico in situ y fuera de horario para nuestros dispositivos y sistemas propiedad del distrito y soportados. No podemos ofrecer el mismo nivel de apoyo a los dispositivos y sistemas BYOD/personales, lo que podría conducir a más tiempo de inactividad del portátil y la pérdida de oportunidades de aprendizaje. Esta práctica es similar a la del sector privado, donde los empleados reciben un dispositivo propiedad de la empresa para garantizar una experiencia de usuario predecible y un soporte técnico óptimo.

Igualdad: algunas familias no pueden permitirse el último portátil o incluso ni siquiera un portátil. Si todos los estudiantes utilizan el mismo dispositivo estándar brindado por el distrito, pueden centrarse en lo que están aprendiendo con el dispositivo, no en quién tiene qué dispositivo y qué más hay en él. Los estudiantes pueden traer sus dispositivos móviles/portátiles a la escuela, sin embargo, los estudiantes que traen sus propios portátiles:

- Deben traer también su portátil del distrito completamente cargado y disponible para su uso
- Deben utilizar el dispositivo del distrito cuando el maestro lo requiera
- Pueden acceder a Internet sólo a través de la red inalámbrica de invitados, donde los filtros están configurados al nivel de protección necesario para un estudiante de primaria.
- No pueden acceder a la impresión o cargar su portátil en la escuela
- Lo hacen bajo su propio riesgo. El distrito no se hace responsable de la pérdida o el robo de portátiles.

¿Qué pasa si no firmo el acuerdo? No quiero que mi familia se haga responsable del portátil.
Si ningún padre o tutor firma o reconoce electrónicamente el acuerdo, el estudiante seguirá teniendo acceso a un portátil cuando esté en la escuela. Si el estudiante daña intencionadamente el portátil, recibirá medidas disciplinarias. Si no hay otro portátil en casa, el estudiante puede estar en desventaja para completar y/o entregar los deberes.

¿Los estudiantes pueden conectarse a la impresora de su casa o cómo pueden hacerlo?
Para instalar una impresora en casa, siga estos pasos:

1. Haga clic en el botón Inicio de Windows y escriba **Dispositivos e Impresoras** y pulse **Intro**
2. Haga clic en **'Agregar una impresora'**
3. Aparece el cuadro Añadir un dispositivo. Elija su impresora y seleccione **Siguiente**
4. Cuando el portátil haya terminado de añadir la impresora, haga clic en **Imprimir una Página de Prueba** y/o en **Finalizar**

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

- Visite el sitio web del fabricante de su impresora y descargue el controlador. Sólo debe descargar la versión de "sólo controlador" del software, ya que el dispositivo no le permitirá instalar el software de gestión de impresión
- Tenga en cuenta la ubicación/carpeta en la que guarda el controlador
- Tenga en cuenta que las impresoras inalámbricas y de red requieren pasos adicionales y posiblemente software que están fuera del alcance de este documento y pueden requerir el apoyo técnico del fabricante. También tenga en cuenta que los estudiantes no están autorizados a instalar software que no sean los controladores de impresión en su portátil, por lo que las impresoras que requieren software de gestión de impresión pueden no ser compatibles con el dispositivo.

Los estudiantes tienen bloqueada la instalación de software por razones de seguridad, lo que también bloqueará la instalación de software de gestión de impresión. Consulte con el fabricante para ver si ofrece una solución de sólo controladores.

Como medida adicional, en casa, los padres pueden añadir filtros a su red doméstica. Una opción es utilizar un servicio de filtrado gratuito como el de http://www.opendns.com/que filtrará el contenido inapropiado de su red doméstica en todos los dispositivos, incluido el dispositivo MAS de LWSD.

¿Cómo puedo entrar en el dispositivo MAS para añadir mi configuración de seguridad de red doméstica personalizada?

Por razones de seguridad, el Distrito no da a los estudiantes o a los padres derechos de administrador de los dispositivos. Configuramos los dispositivos MAS para que funcionen con la seguridad común brindada por la mayoría de las redes inalámbricas que se encuentran en empresas, bibliotecas u hoteles.

Si la seguridad inalámbrica de su hogar es más compleja, podemos ofrecer las siguientes recomendaciones:

1. Añada un segmento a su red con menos seguridad para que lo utilice el dispositivo MAS
2. Conecte el dispositivo MAS directamente a la red doméstica y evite la conexión inalámbrica
3. Abra un hotspot para que lo utilice el dispositivo MAS separado de su red inalámbrica segura
4. Considere la posibilidad de utilizar la configuración de seguridad estándar
5. Considere la posibilidad de añadir seguridad o filtrado a su dispositivo de red, no al portátil, como la oferta de www.opendns.com

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

Estamos obligados por la Ley de Protección de los Niños en Internet (CIPA) de filtrar el contenido de Internet a cualquier dispositivo accedido por los estudiantes en la red LWSD, incluyendo los dispositivos MAS. A algunos estudiantes no les gustan los filtros. Si se les da la oportunidad, los estudiantes podrían instalar un software que anule la seguridad para eludir este requisito. Algunos estudiantes podrían tener la tentación de utilizar los dispositivos para compartir archivos ilegales. Todas estas acciones infringen la Política de Uso Aceptable del distrito.

Recursos de Seguridad en Internet

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

HOJA DE CONSEJOS PARA LA FAMILIA **ESCUELA SECUNDARIA**

Common Sense sobre la
Cultura de la Conectividad

¿Cuál es el problema?
Todos formamos parte de comunidades. Nuestros colegios, nuestras ciudades, nuestras aficiones o intereses forman los centros en torno a los cuales nos relacionamos con otras personas. Todas estas comunidades tienen códigos de comportamiento (escritos o no) que ayudan a que todos se lleven bien. Pero en el mundo digital de hoy, que funciona las 24 horas del día, también formamos parte de comunidades en línea y estas comunidades nos conectan con personas que quizá no conozcamos. Nos conectan en formas en las que sólo nos conocen por nombre de pantalla o donde somos anónimos. Nos conectan con personas que a veces están muy lejos. Ya sea que estemos leyendo o escribiendo la reseña de un restaurante en línea, publicando algo en una página de Facebook, enviando un mensaje de texto a un amigo o compartiendo una foto en un sitio web de fotografía, participamos 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 ya sea a distancia o a través de un nombre de pantalla, esto puede influir en la forma en la que se comportan. Las acciones pueden permanecer ocultas o puede no haber consecuencias. Cuando algo ocurre de forma anónima, es más fácil que la gente se comporte de forma irresponsable, cruel o poco ética. Los niños se benefician de un código de conducta para la actividad en línea y móvil, al igual que necesitan un código de conducta en el mundo real. Deben recibir capacitación para ser buenos ciudadanos digitales, además de ser buenos ciudadanos en general. Nuestros hijos están creando comunidades en línea con cada clic o cada texto que envían y tendrán que vivir en esas comunidades. La información que publiquen sobre ellos mismos o sobre otros durará mucho tiempo y recorrerá grandes distancias. Por eso, 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 su comportamiento en línea es realmente importante para ellos, para sus amigos y para las comunidades más amplias en las que participan. Por último, hay mucho en juego. Cuando los niños hacen un mal uso de la tecnología online o móvil para acosar, avergonzar o intimidar a otros, pueden causar un daño real y duradero.

Common Sense dice

La cultura de la conectividad puede ser positiva o negativa: es lo que la gente hace de ella. Al guiar a nuestros hijos, es importante que entiendan que pueden elegir en todas sus relaciones en línea. Pueden decir algo positivo o decir algo negativo. Pueden crear un gran apoyo comunitario en torno a actividades o intereses, o pueden abusar de la naturaleza pública de las comunidades en línea para dañar a otros.
Hablemos del ciberacoso: Es real. Está en todas partes. Recuerde que los niños a veces cuentan los problemas de un supuesto amigo en lugar de sus propias experiencias. Asegúrese de que sus hijos saben cómo enfrentarse al ciberacoso y que, si la situación se agrava, les recomiende contárselo a un adulto de confianza.
Brinde a los niños un vocabulario sobre el ciberacoso. Hable de los acosadores, de las víctimas, de los espectadores pasivos (aquellos que ven el comportamiento ofensivo, pero no hacen nada para detenerlo) y los "defensores" (personas que intentan activamente detener el ciberacoso). Esto les ayudará a entender qué papel desempeñan o podrían desempeñar.
Fomente las publicaciones positivas. ¿Son sus hijos fans de YouTube? ¿Ellos han dicho algo alentador sobre algo que han visto y les ha gustado? ¿Han aportado conocimientos a un wiki o han compartido su experiencia en un sitio de interés? Desde las edades más tempranas, los niños deben saber que pueden aportar algo positivo al mundo en línea.
Recuérdeles que los mensajes de texto y los mensajes instantáneos pueden no ser persistentes, pero siguen teniendo impacto. Cualquier cosa que digan o hagan con sus teléfonos o a través de mensajes rápidos pueden parecer efímeros cuando los dispositivos se apagan, pero el impacto en los demás permanece, ya sea para bien o para mal.

HOJA DE CONSEJOS PARA LA FAMILIA — **ESCUELA SECUNDARIA Y PREPARATORIA**

Common Sense sobre el Ciberacoso

¿Cuál es el problema?

El ciberacoso es el uso de las herramientas de los medios digitales, como Internet y los teléfonos móviles, para humillar y acosar deliberadamente a otros, a menudo de forma repetida. Aunque la mayoría de los adolescentes no lo hacen, los que lo hacen suelen estar motivados por un deseo de poder, estatus y atención y sus objetivos suelen ser personas con las que compiten por por su posición social. Los ciberacosadores suelen aprovechar el anonimato de la red para dañar a alguien sin ser reconocidos.

El ciberacoso puede adoptar diversas formas, como acosar a alguien, hacerse pasar por otra persona, difundir rumores o enviar información que haga sentir mal a una persona. Los comentarios malintencionados de un acosador pueden difundirse ampliamente a través de la mensajería instantánea, los mensajes de texto telefónicos y las publicaciones en las redes sociales. Esto puede ocurrir rápidamente, con poco tiempo para que los adolescentes reflexionen acerca de las respuestas y puede ocurrir en cualquier momento -en la escuela o en casa- y a menudo implica grandes grupos de adolescentes.

¿Por qué es importante?

El ciberacoso es similar al acoso presencial, pero las herramientas en línea magnifican el daño, la humillación y el drama social de una manera muy pública. Ya sea creando una página falsa de Facebook o MySpace para hacerse pasar por un compañero, enviar repetidamente mensajes de texto e imágenes hirientes, o difundir rumores o publicar comentarios crueles en Internet, el ciberacoso puede provocar graves daños emocionales e incluso físicos.

Aunque cualquiera puede detectar el comportamiento de acoso en el mundo real, es mucho más difícil detectarlo en el mundo en línea. A veces, todo un círculo social se involucra y entonces es más difícil para un adolescente desvincularse de él individualmente. De hecho, grupos enteros de adolescentes pueden participar activa o pasivamente y la víctima puede sentir que es imposible que los acosadores lo dejen en paz. Además, la información hiriente que se publica en Internet es extremadamente difícil de eliminar y millones de personas pueden verla.

Los siguientes consejos pueden ayudarle a reconocer las señales de advertencia del ciberacoso y servirle de guía para hablar con sus hijos adolescentes sobre cómo evitarlo.

Lo que las familias pueden hacer

Pareces deprimido. ¿Ocurre algo en la escuela? ¿Hay algún problema en Internet?
Yo estoy aquí para ti y tus amigos también. Puedes hablar conmigo cuando quieras.
¿Hay algún maestro en la escuela que haya enfrentado este tipo de situaciones antes?
Creo que deberías contarle a uno de ellos lo que está pasando.
Los acosadores quieren atención, poder y estatus, lo que explica por qué necesitan causar drama.
He visto una noticia sobre un adolescente que fue acosado en Internet. ¿Qué harías en esa situación?

LITERACIDAD Y CIUDADANÍA DIGITAL EN LA CULTURA DE LA CONECTIVIDAD
© 2012 www.commonsense.org