Distrito Escolar del Área de Carlisle
Directrices para el uso aceptable de las tecnologías (Política de la Junta #815)
Revisado en julio de 2022

Estudiantes, maestros, personal, voluntarios, estudiantes de maestros, consultores, presentadores e invitados

I. Propósito

El acceso a diversas formas de tecnología, incluyendo Internet, computadoras y otra tecnología en red, es para facilitar el aprendizaje, la enseñanza y las operaciones diarias a través de las comunicaciones interpersonales y el acceso a la información, la investigación y la colaboración. El distrito ha desarrollado pautas cuidadosamente consideradas para garantizar que los recursos del distrito no se utilicen indebidamente y que los sistemas informáticos se utilicen solo para fines legítimos y autorizados. Estas pautas están respaldadas por la Política 815 de la Junta, que se puede ver en www.carlisleschools.org/AUPPolicy815.

El distrito proporciona a los estudiantes, al personal y a otras personas autorizadas acceso a dispositivos propiedad del distrito, sistemas de comunicación electrónica y la red del distrito, que incluye acceso a Internet. Con Internet también viene la disponibilidad de material que puede no ser de valor en el contexto del entorno escolar. El distrito cree firmemente que la valiosa información e interacción disponible en esta red mundial supera con creces la posibilidad de que los usuarios puedan adquirir material que no sea consistente con los objetivos educativos del distrito.

II. Definición

La tecnología del distrito incluye todas las computadoras (computadoras de escritorio y portátiles), tabletas (iPads), periféricos, software, dispositivos de almacenamiento de datos, dispositivos de red de área local y amplia, Internet para incluir todas las aplicaciones en línea a las que se puede vincular la red escolar, todos los datos almacenados en las tecnologías del distrito y todos los demás recursos en red.

III. Autoridad

La disponibilidad de acceso a la información electrónica no implica la aprobación por parte del distrito del contenido, ni el distrito garantiza la exactitud de la información recibida. El distrito no será responsable de ninguna información que pueda perderse, dañarse o no estar disponible al usar la red o de cualquier información que se recupere a través de Internet.

El distrito no será responsable de ningún cargo o tarifa no autorizada que resulte del acceso a Internet u otros recursos de la red.

Los recursos informáticos y de red del distrito son propiedad del distrito. Los usuarios no tendrán ninguna expectativa de privacidad en nada de lo que creen, almacenen, envíen, reciban o muestren en o a través de Internet, computadoras o recursos de red del distrito, incluidos archivos personales o cualquier uso de Internet, computadoras o recursos de red del distrito, ya sea dentro o fuera de la propiedad del distrito. El distrito se reserva el derecho de monitorear, rastrear y registrar el acceso y uso de la red; supervisar la utilización del espacio del servidor de archivos por parte de los usuarios del distrito; o denegar el acceso para evitar actividades no autorizadas, inapropiadas o ilegales y puede revocar los privilegios de acceso y / o administrar las medidas disciplinarias apropiadas. El distrito cooperará en la medida legalmente requerida con el proveedor de servicios de Internet, los funcionarios locales, estatales y federales en cualquier investigación relacionada con el uso indebido de Internet, computadoras y recursos de red del distrito.

El distrito se reserva el derecho de confiscar tecnologías que puedan usarse de manera maliciosa en la red del distrito.

El distrito se reserva el derecho de restringir el acceso a cualquier sitio de Internet o funciones que considere inapropiadas mediante el uso de software y / o bloqueo de servidores en línea. Específicamente, el distrito opera y hace cumplir una (s) medida (s) de protección tecnológica que bloquea o filtra el acceso a material inapropiado por parte de menores en sus computadoras utilizadas y accesibles para adultos y estudiantes. Sin embargo, en una red global, es imposible controlar

todos los materiales y un usuario laborioso puede descubrir información controvertida. La medida de protección tecnológica se aplicará durante el uso de ordenadores con acceso a Internet.

IV. Directrices para el uso aceptable

Cualquiera o todos los usos de las tecnologías definidas están destinados a actividades comerciales y / o educativas autorizadas por estudiantes, padres, profesores y comunidad. Las tecnologías no están destinadas para uso personal.

Los estudiantes, el personal y otras personas autorizadas tienen la responsabilidad de respetar y proteger los derechos de todos los demás usuarios en el distrito y en Internet.

Las cuentas de red solo serán utilizadas por el propietario autorizado de la cuenta para su propósito aprobado. Los usuarios de la red respetarán la privacidad de otros usuarios del sistema.

Cualquier usuario que determine que puede haber un mal uso de la tecnología dentro de la organización, reciba comunicaciones electrónicas amenazantes o no deseadas o visite o acceda inadvertidamente a un sitio inapropiado deberá informarlo inmediatamente a un maestro, director, supervisor o al Director de Tecnología de inmediato.

> Información de la escuela secundaria solo para clases de tecnología CTE: Es posible que se requiera que los estudiantes descarguen software a su directorio de red para usarlo en computadoras en estas aulas del curso. Los estudiantes en estos cursos pueden ser instruidos para configurar sistemas operativos, mover hardware e instalar software como parte del plan de estudios específico del curso. Estas actividades solo pueden ocurrir según lo indicado por el instructor del curso durante el tiempo de clase en computadoras del aula que no están conectadas a la red del distrito.

Prohibiciones

Se espera que los usuarios actúen de manera responsable, ética y legal de acuerdo con la política del distrito, las reglas aceptadas de etiqueta de la red y las leyes federales y estatales. En concreto, se prohíben los siguientes usos:

1. Facilitar la actividad ilegal.
2. Fines comerciales o con fines lucrativos.
3. Trabajo no laboral o no relacionado con la escuela.
4. Publicidad de productos o cabildeo político.
5. Bullying/Cyberbullying.
6. Correo de odio, comentarios discriminatorios y comunicación ofensiva o inflamatoria.
7. Instalación, distribución, reproducción o uso no autorizados o ilegales de materiales protegidos por derechos de autor.
8. Acceder, enviar, recibir, transferir, ver, compartir o descargar materiales, imágenes o fotografías obscenas, pornográficas, lascivas o ilegales.
9. Acceso de estudiantes y menores a material que sea perjudicial para menores o que se determine inapropiado para menores de acuerdo con la política de la Junta.
10. Lenguaje inapropiado o blasfemias.
11. Transmisión de material que pueda ser ofensivo u objetable para los destinatarios.
12. Obtención o modificación intencional de archivos, contraseñas y datos pertenecientes a otros usuarios.
13. Suplantación de identidad de otro usuario, anonimato y seudónimos.
14. Copia, comunicación o modificación fraudulenta de materiales en violación de las leyes de derechos de autor.
15. Cargar o usar juegos, programas, archivos u otros medios electrónicos no autorizados.
16. Interrupción del trabajo de otros usuarios.
17. Destrucción, modificación, abuso o acceso no autorizado al hardware, software y archivos de la red.
18. Acceder a Internet, computadoras del distrito u otros recursos de red sin autorización.
19. Deshabilitar o eludir el software de bloqueo/filtrado de Internet sin autorización.
20. Acceder, enviar, recibir, transferir, ver, compartir o descargar información confidencial sin autorización.

21. Cualquier acción, dentro o fuera del campus, que cause, o sea razonablemente previsible que cause una interrupción sustancial del entorno escolar.

Seguridad

La seguridad del sistema está protegida mediante el uso de contraseñas. Si no se protegen o actualizan adecuadamente las contraseñas, se podría lograr el acceso no autorizado a los archivos personales o del distrito. Para proteger la integridad del sistema, se seguirán estas directrices:

1. Los empleados y estudiantes no revelarán sus contraseñas a otra persona.
2. Los usuarios no deben usar un equipo que haya iniciado sesión con el nombre de otro usuario.
3. A cualquier usuario identificado como un riesgo de seguridad o que tenga un historial de problemas con otros sistemas informáticos se le puede negar el acceso a la red.

Todos los empleados, estudiantes y voluntarios aprobados tienen obligaciones bajo la ley federal para proteger la información de identificación personal de los estudiantes y cierta información personal de los empleados de cualquier acceso, divulgación o divulgación no autorizados. Los empleados, estudiantes y voluntarios aprobados deben cumplir con todas las leyes aplicables y deben tener precaución y utilizar medidas de seguridad adecuadas, como la protección con contraseña en sus dispositivos electrónicos, para evitar cualquier acceso no autorizado a datos confidenciales. En ningún caso los empleados almacenarán datos confidenciales localmente en el disco duro o la memoria interna del dispositivo electrónico personal del empleado. Los datos confidenciales solo pueden almacenarse en recursos emitidos y / o controlados por el distrito. Los datos confidenciales nunca deben almacenarse en dispositivos personales o periféricos.

Software/Aplicaciones

Todo el software debe utilizarse de acuerdo con su acuerdo de licencia. La infracción de derechos de autor del software es ilegal. La ley que rodea la infracción de derechos de autor afecta no solo al individuo infractor sino también al distrito. Cualquier pregunta o inquietud con respecto a la legalidad del software debe remitirse al Director de Tecnología.

Todo el software utilizado por el distrito en las computadoras propiedad del distrito se comprará a través del departamento de tecnología. Todo el software debe entregarse al departamento de tecnología para completar los requisitos de registro e inventario. El software debe estar registrado a nombre del Distrito Escolar del Área de Carlisle e incluirá el título del trabajo o el departamento en el que se utilizará.

Todo el software será autorizado e instalado por el departamento de tecnología. El departamento de tecnología puede aprobar a otros usuarios para instalar un programa de software específico en una computadora específica. Una vez instalado el software, los medios originales se mantendrán en un área de almacenamiento mantenida por el departamento de tecnología.

Puede encontrar una lista de aplicaciones aprobadas instaladas en tabletas (iPads) en www.carlisleschools.org/apps.

Los usuarios no distribuirán software a personas externas, incluidos consultores, capacitadores, estudiantes de maestros o cualquier contacto personal.

Ningún software, shareware, software gratuito, servicio web, aplicación portátil u otro archivo ejecutable no autorizado puede descargarse, copiarse, usarse o guardarse en ningún dispositivo tecnológico propiedad del distrito, sin el permiso previo del Director de Tecnología.

Hardware y tecnologías periféricas

Los dispositivos personales (incluidos teléfonos celulares, impresoras, computadoras portátiles, etc.) deben utilizarse a riesgo del propietario. No es responsabilidad del distrito reparar o reemplazar el dispositivo en los casos en que el dispositivo esté dañado, perdido, robado, no funcione correctamente o sea incompatible. El distrito se reserva el derecho de desconectar dispositivos personales o deshabilitar servicios sin previo aviso.

Se prohíbe el uso de equipos de red personal en el sitio sin recibir permiso del Director de Tecnología. Además, no se permite que ningún dispositivo personal esté cableado (*conectado mediante cable Ethernet*) a la red CASD.

Ningún equipo se moverá entre aulas, oficinas y edificios ni se desechará sin el permiso previo del Director de Operaciones de TI.

Todos los usuarios deben hacer esfuerzos razonables para protegerse contra el robo o daño del equipo del distrito. Los dispositivos tecnológicos que se dejan desatendidos deben estar asegurados.

No se pueden realizar alteraciones, actualizaciones o modificaciones en el hardware a menos que lo apruebe el Director de Operaciones de TI.

Los medios personales como discos de datos, CD, DVD y dispositivos USB se pueden usar para transferir archivos que están directamente relacionados con la tarea del aula o la función administrativa. Cualquier otra transferencia de archivos entre la red del distrito y los medios personales está estrictamente prohibida.

Todos los suministros de tecnología del distrito, incluidos el papel, la tinta y los medios de comunicación, deben utilizarse únicamente con fines educativos, administrativos y comerciales.

El distrito no es responsable de la pérdida o daño de cualquier dispositivo electrónico que un empleado o estudiante traiga a la escuela, actividades extracurriculares o eventos o viajes patrocinados por la escuela.

Red, incluido el uso de Internet y correo electrónico
Las cuentas de red son creadas por el departamento de tecnología y son propiedad del Distrito Escolar del Área de Carlisle. Los estudiantes y el personal son responsables de mantener una contraseña confidencial para su cuenta.

El personal debe cambiar su contraseña no menos de cada seis meses utilizando las pautas de contraseña publicadas en la unidad compartida del distrito.

Los usuarios no pueden compartir sus contraseñas de cuenta de red o aplicación con nadie. Esto se aplica a todos los programas, bases de datos y sistemas basados en la web, incluidos, entre otros, los sitios web del distrito y de maestros, PowerSchool, PowerTeacher,
Schoology, Seesaw, USA Test Prep, 4Sight, GRADE, Dibels y todas las solicitudes del Departamento de Educación de Pensilvania.
Los estudiantes de magisterio y los sustitutos del día a día deben usar el inicio de sesión de PowerTeacher Substitute para tomar asistencia en
PowerTeacher. A los sustitutos a largo plazo se les asignará su propio inicio de sesión para PowerTeacher y la red.
Estudiante
Los maestros <u>no están</u> autorizados a acceder a PowerTeacher para ingresar calificaciones, ya que ese acceso se otorga a un maestro específico.

Los dispositivos personales que se utilizan para acceder a los recursos del distrito, como el correo electrónico, los sistemas de información de los estudiantes y otros recursos en línea, deben estar protegidos con contraseña.

Los usuarios son responsables de cerrar la sesión correctamente al final de una sesión y bloquear la computadora si está fuera de la vista de la computadora durante cualquier período de tiempo. Los usuarios serán responsables de todas las acciones realizadas bajo su cuenta de usuario.

<u>Pizarra interactiva, TV, proyector:</u> Cuando un miembro del personal está llevando a cabo una actividad grupal utilizando la SmartBoard, los estudiantes pueden interactuar con la actividad bajo la supervisión directa del personal. El miembro del personal debe participar activamente en la lección. El uso de dispositivos de esta

manera no está permitido si un estudiante está trabajando de forma independiente o el miembro del personal está trabajando en otro lugar o circulando por la sala.

Cada usuario tendrá acceso a una cuenta de Microsoft 365 y/o a una unidad iCloud para almacenar archivos. Los usuarios no deben guardar archivos en el equipo local. Los usuarios deben administrar su sistema de almacenamiento de archivos y correo electrónico eliminando archivos que estén desactualizados o sean innecesarios y que no sean necesarios a través de una directiva de retención de registros. Todo el personal es responsable de preservar los archivos según lo requerido por la política de retención de registros del distrito.

Los usuarios no pueden intentar ver o configurar la red, los archivos o los programas. Todos los usuarios deben notificar inmediatamente al departamento de tecnología de cualquier violación, sospecha de violación o posible violación de la seguridad de la red. El usuario no demostrará el problema a nadie fuera del departamento de tecnología.

El personal guardará y organizará archivos y correos electrónicos, que de otro modo se mantendrían en una carpeta de registros de estudiantes o en un archivo de personal como se indica en la política de retención de registros del distrito. El personal no divulgará ni divulgará información de identificación personal sobre los estudiantes, excepto de acuerdo con la Ley de Privacidad de los Derechos Educativos de la Familia (FERPA) y la política de registros estudiantiles del distrito.

El sonido, la música, el video o cualquier otro archivo multimedia al que se acceda a través de las tecnologías del distrito deben estar directamente relacionados con una asignación del distrito.

El acceso a los sitios web de redes sociales es solo para fines educativos y según lo asignado por un maestro o supervisor de personal.

El acoso cibernético, crear una amenaza para un estudiante, miembro del personal o cuando está en el entorno escolar, que tiene el efecto de hacer cualquiera de los siguientes: interferir sustancialmente con la educación de un estudiante, crear un ambiente amenazante y / o interrumpir sustancialmente el funcionamiento ordenado de la escuela está prohibido. Consulte la Política 249 de la Junta en https://www.carlisleschools.org/Policy249.

Si un usuario accede u observa accidentalmente material que es objetable, obsceno, ilegal o inapropiado, debe notificar inmediatamente al maestro supervisor o supervisor. Estos sitios deben ser reportados al Director de Tecnología.

Los usuarios no deben divulgar información personal al personal que no pertenece al distrito, como domicilio, descripción física, ruta hacia y desde la escuela, o cualquier otra información que pueda amenazar la seguridad de los estudiantes o el personal.

Las cuentas de correo electrónico se asignan a los empleados del distrito. Los maestros estudiantes y los empleados contratados deben usar la dirección de correo electrónico de su universidad o empresa para comunicarse con el personal del distrito a través de un servicio basado en la web.

Los usuarios no deben reenviar spam o correo electrónico no relacionado con el trabajo a ninguna otra cuenta del distrito o no del distrito.

Videoconferencia

Las herramientas de videoconferencia pueden ser un recurso valioso para el aprendizaje virtual y otras oportunidades para que los estudiantes, el personal, los padres y los miembros de la comunidad se reúnan fuera de un espacio físico. Toda la comunicación (a través de audio, video, imágenes fijas, etc.) y el comportamiento en una videoconferencia siguen las mismas expectativas que en el entorno escolar presencial regular.

Acceso a Internet
El distrito ha instalado un software de filtrado de sitios de Internet para evitar que los usuarios de la red accedan a sitios que son inapropiados para uso educativo. El software de filtrado se instala en todos los dispositivos estudiantiles propiedad del Distrito para el filtrado de Internet para el acceso dentro y fuera del campus. El fabricante del software actualizará periódicamente el filtrado para incluir los sitios recién descubiertos que sean inapropiados. El departamento de tecnología, en coordinación con la administración, también evaluará y, si es necesario, bloqueará el acceso a los sitios reportados y anulará los sitios bloqueados que se consideren apropiados. Los usuarios no pueden usar software, alterar la configuración del proxy o usar cualquier otro medio para eludir el filtro del distrito.

Consecuencias del uso inadecuado
El usuario de la red será responsable de los daños al equipo, sistemas y software que resulten de actos deliberados o intencionales.

Uso ilegal de la red; eliminación intencional o daño a archivos o datos pertenecientes a otros; violaciones de derechos de autor; y el robo de servicios se denunciará a las autoridades judiciales competentes para su posible enjuiciamiento.

Las reglas generales de comportamiento y comunicaciones se aplican cuando se utiliza Internet o cualquier aplicación con opciones de mensajería, además de las estipulaciones de esta política.

El distrito se reserva el derecho de promulgar medidas disciplinarias de acuerdo con las políticas de los empleados o las pautas de conducta de los estudiantes por el uso inapropiado, no autorizado o ilegal de las tecnologías. Para los estudiantes, la acción disciplinaria puede incluir suspensión o expulsión. Para el personal, las medidas disciplinarias pueden incluir la suspensión o el despido. El distrito se reserva el derecho de cobrar al usuario por los costos de reparación o reemplazo de dichas tecnologías.

El vandalismo está prohibido y los usuarios serán responsables de cualquier costo asociado con dicho acto. El vandalismo incluye la destrucción o modificación del hardware, así como cualquier intento malicioso de dañar o destruir datos de otro usuario, Internet u otras redes; Esto incluye, entre otros, cargar o crear virus informáticos. El vandalismo puede resultar en la pérdida de privilegios de acceso, medidas disciplinarias y / o procedimientos legales.

V. Garantías
El distrito no ofrece garantías de ningún tipo, ya sean expresas o implícitas, por los servicios que proporciona. El distrito no será responsable de los daños que sufra un usuario. Esto incluye la pérdida de datos resultante de retrasos, no entregas, entregas erróneas o interrupciones del servicio causadas por la negligencia del distrito o por errores u omisiones del usuario. El uso de cualquier información obtenida a través de Internet es bajo el propio riesgo del usuario. El distrito niega específicamente cualquier responsabilidad por la exactitud o calidad de la información obtenida a través de sus servicios. Todos los usuarios deben considerar la fuente de cualquier información que obtengan y considerar cuán válida puede ser la información.

El distrito no será responsable de los cargos o tarifas no autorizados que resulten del acceso a Internet. Toda la responsabilidad financiera recaerá en el empleado o estudiante individual que incurra en cargos o tarifas no autorizados.