Distrito Escolar de la Ciudad de Provo
Norma Serie 4000: Plan de Estudios, Enseñanza, Evaluación

4202 P2

El propósito de la traducción de este material al idioma Español, es proveer una herramienta de apoyo al público en general que no habla Inglés, pero pueden existir diferencias en la traducción.

Recursos Electrónicos: Empleados, Voluntarios, Usuarios Invitados

Los siguientes procedimientos están escritos para apoyar a la norma de Recursos Electrónicos y para promover una ciberciudadanía positiva y efectiva entre el personal, los pasantes, visitantes y voluntarios. La ciberciudadanía digital representa más que la alfabetización tecnológica. Afortunadamente, los ciberciudadanos con fluidez tecnológica viven seguros y civilizados en un mundo cada vez más digital. Ellos reconocen que la información publicada en el internet es pública y permanente y puede tener un impacto duradero en la vida y profesión de una persona. En este documento, los términos "personal" y/o "empleado" incluyen a los pasantes, visitantes, voluntarios y empleados del distrito.

Servicios de Red

Como se indica en la norma 4202, "servicios de red" incluyen, pero no se limitan a, computadoras con cable e inalámbricas, dispositivos y equipo periférico, archivos y almacenamiento, correos electrónicos y contenido del internet (blogs, sitios web, correo web, grupos, wikis, etc.). El distrito se reserva el derecho de priorizar y restringir el uso y el acceso a la red.

Los "servicios de red" apoyan a la educación y a la investigación de acuerdo con la misión del distrito. El Distrito Escolar de la Ciudad de Provo posee la red proveída en todo el distrito, junto con todas las computadoras proporcionadas por el distrito; el distrito tiene, por lo tanto, el derecho de regular su uso.

Las comunicaciones en las computadoras y redes del distrito son públicas. No debe presumirse de privacidad ni está garantizada, incluso para mensajes personales. Por lo tanto, el personal:

- No debe incluir en las comunicaciones electrónicas sus direcciones personales, fotos de sí mismos, números de teléfono, ubicación de su escuela, números de seguro social, números de identificación de los empleados ni información financiera personal.
- Debe avisar inmediatamente al administrador del sistema si encuentran materiales que violen las reglas de uso apropiado, o si los mensajes o archivos enviados a ellos contienen amenazas, referencias sexuales o si los hacen sentir incómodos.
- No debe divulgar su contraseña a otra persona.

El uso del sistema debe cumplir con la ley estatal y federal, con las normas y licencias de los proveedores de red y con la norma del distrito. El uso del sistema está prohibido para hacer solicitudes comerciales.

Como una protección a la red del distrito y para administrar las demandas tecnológicas dentro de las restricciones del personal del departamento de tecnología, el distrito se reserva el derecho de negar el acceso al internet/conectividad a la red, a los equipos personales de los que sean dueños y al equipo que no pertenezca al distrito. La conectividad de cualquier dispositivo electrónico personal está sujeto a la revisión del distrito y a todos los lineamientos en este documento.

El uso aceptable de la red incluye:

- La creación de archivos, proyectos, videos, páginas web y archivos de audio digital utilizando los recursos de la red para apoyar la investigación educativa;
- La participación en blogs, wikis, tablones de anuncios, sitios de redes sociales y grupos y la creación de contenido para archivos de audio digital, correo electrónico y páginas web que apoyen la investigación educativa;
- La publicación en línea de material educativo original;
- Los materiales relacionados con el plan de estudios y trabajo de los estudiantes (las fuentes fuera del aula o de la escuela deben ser citadas apropiadamente); y
- El acceso a los recursos de cloud (almacenamiento) como correo electrónico, archivos compartidos y otros servicios educativos.

El uso inaceptable de la red incluye pero no está limitado a:

- La ganancia personal, solicitudes comerciales y compensación de cualquier tipo;
- La responsabilidad o costo incurrido por el distrito;
- La descarga, instalación y uso de juegos, archivos de audio, archivos de video u otras aplicaciones (incluyendo “shareware” las aplicaciones gratuitas de prueba que requieren posteriormente de pago o “freeware” las aplicaciones gratuitas) excepto cuando se hayan aprobado previamente por el director de la escuela, administrador, o por el departamento de tecnología;
- El apoyo u oposición para las medidas de votación, candidatos y cualquier otra actividad política;
- El uso de lenguaje obsceno, vulgar o inapropiado;
- Piratear, golpear, destruir, inhabilitar el software del antivirus, la introducción de virus, gusanos, malware (software destinado a dañar o deshabilitar las computadoras y los sistemas informáticos), caballos de Troya (programa diseñado para romper la seguridad de un sistema informático mientras que aparentemente realiza alguna función inocua), bombas de tiempo, escaneo en red, etc. y la realización de cambios al hardware, software y herramientas de monitoreo;
- El acceso no autorizado a los servidores del distrito, computadoras, dispositivos electrónicos, equipos de red y sistemas de información;
- Los daños físicos a las computadoras, sistemas informáticos o a la red de computadoras;
- La intimidación cibernética, correos hostiles, difamación, calumnias, acoso de cualquier tipo, bromas/observaciones/imágenes discriminatorias;
- La información publicada, enviada o almacenada en línea que pudiera poner en peligro a otros (por ejemplo, construcción de bombas, fabricación de medicamentos/drogas);
- Usar el equipo de cualquier manera que sea inconsistente con las normas individuales de la escuela;

- Evitar que los filtros del internet o de correo electrónico tengan acceso a contenido que no sea conforme a CIPA. (CIPA – Ley de Protección del Internet para Niños);
- Poseer en la escuela o en cualquier actividad relacionada con la escuela, cualquier material pornográfico o sexualmente explícito en cualquier forma en cualquier dispositivo personal o del distrito; (los servicios de almacenamiento en cloud como dropbox, copias, y sugarsync (servicio de sincronización de archivos en línea) colocando copias digitales de archivos en su dispositivo);
- Violar las leyes de derechos de autor;
- Compartir las contraseñas o conceder acceso al servicio de red del distrito iniciando una sesión para los estudiantes, usuarios o empleados;
- Usar su contraseña para autorizar información del distrito que no sea directamente necesaria para cumplir con sus responsabilidades actuales;
- Meterse sin derecho en las carpetas, trabajos o archivos de otros (los oficiales de la escuela pueden monitorear las carpetas, trabajos o archivos sin permiso o aviso);
- Interrumpir intencionalmente el sistema o desperdiciar los recursos en cualquier manera (como el espacio en disco, la capacidad de impresión o la intromisión electrónica);
- Acceso, carga, descarga, almacenamiento y distribución de material obsceno, pornográfico o sexualmente explícito; y
- Agregar equipo no autorizado a la red del distrito. Cualquier equipo de este tipo pudiera ser confiscado.

El uso de los servicios de red es un privilegio, no un derecho. El uso inapropiado resultará en la cancelación de esos privilegios y posiblemente en otras acciones disciplinarias o legales incluyendo persecución penal, suspensión, expulsión o la terminación del empleo.

Seguridad del Internet

Información Personal y Contenido Inapropiado:

- El personal no debe revelar información personal de los estudiantes, fotos/videos de ellos ni del personal, incluyendo una dirección de casa y número de teléfono, en sitios web, blogs, archivos de audio digital, videos, wikis, correos electrónicos o como contenido en cualquier otro medio electrónico.
- El personal no debe revelar información personal sobre otro individuo en ningún medio electrónico.
- No se pueden publicar fotos, videos o nombres de los estudiantes en ninguna clase, escuela o sitio web del distrito a menos que el permiso apropiado haya sido cotejado de acuerdo con las regulaciones de FERPA (Ley de Derechos Educativos y Privacidad Familiar).
- Si los empleados del distrito encuentran información peligrosa o inapropiada o mensajes, deben notificar a la autoridad escolar o del distrito apropiada.

Filtración y Monitoreo

El software de filtración se utiliza para bloquear o filtrar el acceso a las representaciones visuales que son obscenas o pornográficas - y toda la pornografía infantil de acuerdo con la Ley de Protección del Internet para Niños (CIPA). Otro material censurable podría ser filtrado. La determinación de lo que constituye "otro material censurable" es una decisión local. El software

de filtración no es 100 por ciento efectivo. Mientras que los filtros hacen que sea más difícil la recepción o acceso al material censurable, los filtros por sí solos no son una solución.

Reglas de Filtración:

- Cada usuario es responsable de su uso de la red y del internet y debe evitar los sitios censurables;
- Queda prohibido cualquier intento por anular o sobrepasar el filtro del internet del distrito o encubrir la actividad del internet. Estos intentos incluyen, pero no se limitan a, el uso de proxies (servidores de enlace), https (protocolo seguro de transferencia de hipertexto), puertos especiales, modificaciones a la configuración del navegador del distrito y cualquier otra técnica diseñada para evitar la filtración o permitir la publicación de contenido inapropiado;
- Los maestros y el personal proporcionarán la supervisión adulta apropiada al uso del internet.
- El personal debe hacer un esfuerzo razonable para monitorear el uso de este equipo para asegurar que el uso del estudiante se ajuste a la misión y metas del distrito; y
- El personal debe hacer un esfuerzo razonable para familiarizarse con el internet y controlar, enseñar y ayudar eficazmente.

Los filtros bloquean las siguientes categorías:

- El contenido para adultos, el contenido sexualmente explícito, pornografía infantil, pornografía, arte explícito, el contenido obsceno, sin sabor y el contenido clasificado como "R".
- Seguridad: Dominios de mala reputación, BotNet (red de computadoras privadas infectadas con software malicioso y controladas sin el conocimiento del propietario), pirateo, código malicioso, virus, Phishing (envío de correos electrónicos fraudulentos con el fin de que las personas revelen su información personal), Spyware (software que permite al usuario obtener información encubierta sobre las actividades informáticas de otra persona mediante la transmisión secreta de datos desde su hardware), Peer-to-Peer/Filesharing (cada computadora puede actuar como servidor para los demás, permitiendo el acceso compartido a archivos y periféricos sin necesidad de un servidor central), y Proxies/Anonymizers (herramienta que intenta hacer que la actividad en internet no pueda ser rastreada).
- Juegos de azar
- Ilegal / Cuestionable: Habilidades penales, inseguro/desagradable, odio y discriminación,
- Drogas ilegales, hacer trampa en la escuela, terrorista/militante/extremista.
- Alcohol
- Tabaco
- Todas las otras categorías de conformidad con CIPA según sea necesario.

Categorías de excepción:

- Material Educativo: Material bajo otra categoría que tenga un valor educativo (como la literatura clásica, la educación sexual, etc.)

Derechos de Autor

Por lo general, se prohíbe descargar, copiar, duplicar y distribuir software, música, archivos de sonido, películas, imágenes u otros materiales protegidos por los derechos de autor sin el permiso específico del propietario de dichos derechos de autor. Sin embargo, la duplicación y distribución de materiales con fines educativos están permitidos cuando tal duplicación y distribución caigan dentro de la Doctrina del Uso Justo de la Ley de Derechos de Autor de los Estados Unidos (Título 17, USC) y el contenido sea citado apropiadamente.

Todos los trabajos de los estudiantes son tratados como derechos de autor. El permiso para publicar cualquier trabajo de los estudiantes requiere del permiso del padre o tutor.

Seguridad y Privacidad de la Red

Las contraseñas son el primer nivel de seguridad para cualquier cuenta de usuario. Los inicios de sesión del sistema y las cuentas deben ser utilizados únicamente por el propietario autorizado de la cuenta para propósitos autorizados del distrito. Los estudiantes y el personal son responsables de toda la actividad en su cuenta y no deben compartir la contraseña de su cuenta.

Cada persona es responsable de la actividad que ocurra con su contraseña. Los siguientes pasos son necesarios para proteger las cuentas de usuario de la red:

- Cambiar su contraseña regularmente;
- No usar la cuenta de otra persona;
- No enviar contraseñas en un correo electrónico o en otras comunicaciones,
- Si usted escribe la contraseña de su cuenta de usuario, guárdelo en un lugar seguro;
- No guarde las contraseñas en un archivo sin ser encriptado,
- No utilice la opción de “recordar contraseña” en el navegador del internet; y
- Bloquee la pantalla o cierre la sesión, si se aleja de la computadora.

Los datos de los estudiantes son confidenciales. El personal del distrito debe mantener la confidencialidad de los datos de los estudiantes de acuerdo con la Ley de Derechos Educativos y Privacidad Familiar (FERPA).

No Existen Expectativas de Privacidad

El distrito proporciona el sistema de red, correo electrónico y acceso al internet como una herramienta para la educación y la investigación en apoyo con la misión del distrito. El distrito se reserva el derecho de controlar, inspeccionar, copiar, revisar y almacenar, sin previo aviso, la información sobre el contenido y el uso de:

- La red;
- Utilización de los archivos de usuario y espacio en disco;
- Utilización de las aplicaciones de usuario y de ancho de banda;
- Archivos de documentos de usuario, carpetas y comunicaciones electrónicas;
- Correo electrónico;
- Acceso al internet; y
- Toda y cualquier información transmitida o recibida en conexión con la red y con el uso del correo electrónico.

Ningún usuario debe presumir expectativa de privacidad alguna al usar la red, el software o el equipo del distrito. El distrito se reserva el derecho de revelar cualquier mensaje electrónico a las autoridades o a terceros, según corresponda. Todos los documentos están sujetos a las leyes de divulgación de los registros públicos. Para determinar si esta norma ha sido violada durante una investigación, el distrito se reserva el derecho de presentar una solicitud de GRAMA (Ley de Acceso y Gestión de Archivos del Gobierno) para obtener información sobre el teléfono personal y la cuenta personal si el servicio del teléfono/dispositivo es pagado con los fondos del distrito.

Acción Disciplinaria

Todos los empleados están de acuerdo con todas las normas del distrito al momento de ser contratados, y también cuando firmen sus contratos anualmente.

El uso de los "servicios de red" del distrito es un privilegio, no un derecho. El uso inapropiado resultará en la cancelación de esos privilegios y posiblemente en otras medidas disciplinarias incluyendo la suspensión o terminación de su empleo. También pueden ejercerse acciones legales, incluyendo la persecución civil y penal, hacia los individuos que causen daño deliberadamente a la red, equipo y/o servicios relacionados del distrito.

Fecha de Aprobación:	11 de diciembre de 2012
Actualización:	24 de noviembre de 2014