DISTRITO DE ESCUELAS PRIMARIAS DE WESTMORLAND UNION

Política de la Junta Nº 5035: SEGURIDAD DE INTERNET Y USO DE COMPUTADORAS PARA LOS ESTUDIANTES

A. Propósito y cobertura

1. Esta política define el uso apropiado por parte de los estudiantes del Distrito de Escuelas Primarias de Westmorland ("Distrito") de los recursos electrónicos del Distrito, incluyendo, pero no limitado a, sus computadoras, sistemas informáticos y servicios de acceso a Internet.

2. Esta política se aplica a todos los estudiantes del Distrito.

3. El Gerente de Información de Sistemas de Gestión del Distrito será el Superintendente

B. Resumen de la Política con respecto al Uso de los Estudiantes

1. El Distrito proporciona a sus estudiantes recursos electrónicos tales como computadoras para su uso como herramientas educativas. El Distrito reconoce que estos recursos presentan oportunidades tentadoras para que los usuarios obtengan acceso a asuntos que son confidenciales, requieren acceso restringido o que resultan en un uso inadecuado de los recursos del Distrito. Es responsabilidad de cada estudiante asegurarse de que los recursos electrónicos del Distrito se utilicen con fines educativos legítimos y de una manera que no comprometa la información confidencial, patentada o sensible. Los estudiantes no pueden usar ni permitir que otros usen los sistemas informáticos del Distrito u otros recursos electrónicos para propósitos ilegales. Dicha conducta deberá ser reportada y no será tolerada. El mal uso de los sistemas informáticos del Distrito u otros recursos electrónicos resultará en medidas disciplinarias, que pueden incluir la expulsión de la escuela.

2. Los sistemas informáticos del Distrito y otros recursos electrónicos son propiedad del Distrito. Existen numerosas formas en las que el uso indebido de esta propiedad podría poner en peligro el funcionamiento adecuado de los sistemas informáticos del Distrito y exponer al Distrito y sus empleados a responsabilidad en caso de una demanda. Por ejemplo, el uso del sistema informático del Distrito para propósitos no relacionados con el plan de estudios educativo del Distrito compromete la memoria disponible restante de dichos sistemas y puede frenar la capacidad del sistema para procesar datos de manera efectiva u oportuna. Los virus descargados de disquetes personales pueden dañar los sistemas y la información almacenada que es crítica para el desempeño de las responsabilidades del Distrito. El uso de Internet y / o el acceso al correo electrónico proporcionado a los empleados del Distrito para descargar o enviar material obsceno o discriminatorio podría exponer al Distrito y sus empleados a responsabilidad por reclamos de acoso sexual o discriminación. Por estas y otras razones, los estudiantes no tendrán acceso al correo electrónico y el uso de las computadoras por parte de los estudiantes estará bajo la supervisión directa de un empleado certificado en todo momento. Además, se han instalado medidas de protección tecnológica que bloquean o filtran el acceso a representaciones visuales

que sean obscenas, pornografía infantil u otro material perjudicial para los menores, y a las salas de chat. Estas medidas deben estar vigentes durante cualquier uso de cualquier computadora del Distrito por parte de menores.

3. Para garantizar que los sistemas informáticos del Distrito no se utilicen incorrectamente, el Distrito puede inspeccionar y / o monitorear aleatoriamente los archivos de la computadora, los dispositivos de almacenamiento del Distrito como unidades flash y discos, el uso de Internet y toda otra información almacenada o grabada por los estudiantes en los sistemas informáticos para asegurar que estos recursos públicos no sean mal utilizados. Los estudiantes no deben esperar que la información guardada en los sistemas o equipos informáticos del Distrito sea privada, incluso si la información es personal. Los datos informáticos pueden controlarse independientemente de su origen o contenido. Al utilizar los sistemas informáticos del Distrito y otros recursos electrónicos, un estudiante da su consentimiento al monitoreo resumido en esta política. Por la presente, se notifica a los estudiantes que el Distrito no es responsable de ninguna lesión a los estudiantes causada por otras personas que puedan acceder a dicha información.

4. El Distrito se reserva el derecho de tomar cualquier acción para cumplir completamente con las provisiones en 20 USCA sección 6777 (Seguridad en Internet), incluyendo, pero no limitado a, el uso de medidas de protección tecnológica para bloquear el acceso de los estudiantes a sitios web que contienen contenido obsceno, pornográfico u otro material dañino para menores; y el uso de medidas tecnológicas para prevenir la piratería o cualquier actividad ilegal.

C. Definiciones

1. El término "personal" o "información personal" como se usa en esta política se refiere a información no relacionada con las actividades académicas del estudiante, u otra información que el estudiante no quiera divulgar a otros.

2. El término "computadora" incluye cualquier hardware, software u otra tecnología adjunta o conectada, instalada o utilizada de otro modo en conexión con una computadora.

3. El acceso a Internet incluirá todas las computadoras del Distrito conectadas a una red informática y / o Internet, y otros dispositivos de comunicación electrónica personal que accedan a la red del Distrito y / o Internet.

4. El término “pornografía infantil” tiene el significado que se le da a ese término en la jurisprudencia federal y estatal y está prohibido si es obsceno o si representa a niños reales.

5. El término "perjudicial para los menores" significa cualquier fotografía, imagen, archivo de imagen gráfica u otra representación visual que, tomada en su conjunto y con respecto a los menores, apele a un interés lascivo en la desnudez, el sexo o la excreción; que represente, describa o represente, de manera evidentemente ofensiva con respecto a lo que es adecuado para menores, un acto sexual o contacto sexual real o simulado, actos sexuales normales o pervertidos reales o simulados, o una

exhibición lasciva de los genitales; y en su conjunto, carece de valor literario, artístico, político o científico serio en cuanto a los menores.

6. El término "obsceno" tiene el significado aplicable a ese término según la sección 1460 del 18 USC.

7. El término "acto sexual" y "contacto sexual" tienen los significados que se dan en la sección 2246 del Título 18.

D. Acceso prohibido para estudiantes

A los estudiantes solo se les permitirá usar solo las computadoras del Distrito que estén equipadas con dispositivos de protección de tecnología diseñados para evitar el acceso a pornografía infantil, materiales obscenos u otros materiales dañinos para los niños. Los estudiantes deben utilizar computadoras e Internet únicamente bajo la supervisión directa de un empleado certificado del Distrito.

E. Uso inaceptable

1. No se proporcionará acceso al correo electrónico a los estudiantes, excepto a aquellos estudiantes que participen en un programa piloto bajo una subvención de la Fundación Beaumont.

2. El uso de los sistemas informáticos del Distrito y otros recursos electrónicos es un privilegio que puede ser revocado en cualquier momento. Los estudiantes reciben computadoras, archivos de computadora, servicios de Internet, software y otros recursos electrónicos para que los usen en relación con los requisitos educativos del Distrito. Toda la información almacenada o registrada en las computadoras del Distrito se considerará propiedad del Distrito y puede ser recuperada y revisada por el Gerente de Sistemas de Información para asegurar que los recursos informáticos del Distrito no estén siendo mal utilizados. Los estudiantes del Distrito no pueden esperar que la información personal registrada o almacenada en los recursos informáticos del Distrito permanezca privada. El Distrito no tolerará el mal uso de sus recursos electrónicos. La conducta que resultará en la disciplina del estudiante incluirá, pero no se limitará a:

   a. Causar mal funcionamiento, daño o robo del hardware, software o componentes del sistema;

   b. Alterar el software o hardware del sistema;

   c. Colocar información ilegal, virus informáticos o programas dañinos en o a través de los sistemas informáticos;

   d. Entrar en información restringida o correo electrónico en sistemas o archivos de red en violación de esta política;

   e. Violar la privacidad de otros usuarios del sistema informático;

f. Usar el nombre de un empleado para enviar o recibir mensajes en la red o Internet;

g. Violar la Ley de Decencia en las Comunicaciones federal o cualquier otra ley federal o estatal aplicable a los sistemas informáticos y / o de telecomunicaciones;

h. Usar los sistemas informáticos del Distrito u otros recursos electrónicos para beneficio personal, lucro, juegos de azar o con fines comerciales, o para participar en cualquier actividad ilegal;

i. Mostrar o transmitir imágenes, mensajes o dibujos animados sexualmente explícitos que sean obscenos, pornografía infantil o material dañino para menores;

j. Usar el sistema informático del Distrito para acosar ilegalmente a otras personas;

k. Mostrar o transmitir mensajes que contengan insultos étnicos, comentarios raciales, bromas subidas de tono o cualquier cosa que pueda entrar en conflicto con la política del Distrito de proporcionar un entorno educativo sensible a la diversidad y libre de acoso y falta de respeto;

l. Revisión, duplicación, diseminación, remoción, daño o alteración no autorizada de archivos, contraseñas, identificaciones de usuario, sistemas o programas informáticos u otra propiedad del Distrito, una empresa o cualquier agencia gubernamental para realizar actividades comúnmente descritas como "piratería". "

m. Usar datos protegidos por derechos de autor u otros materiales sin el permiso del titular de los derechos de autor, incluido, entre otros, el uso de datos descargados de Internet y la creación o mantenimiento de copias de archivo de materiales obtenidos a través de Internet, a menos que dichos materiales sean de dominio público.

n. Obtener, descargar, ver u obtener acceso a materiales que puedan considerarse ilegales, dañinos, abusivos, obscenos, pornográficos, que describan dispositivos destructivos o que sean materiales dañinos según se define en la sección 313 (a) del Código Penal de California, o que sean de otra manera objetable según las políticas actuales del Distrito o las leyes estatales o federales aplicables.

o. Colocar programas en sistemas informáticos sin el permiso del Distrito.

p. A menos que se haya obtenido la aprobación previa del Gerente de Sistemas de Información, el uso de Internet u otras conexiones de red externas de una manera que podría permitir que personas no autorizadas obtengan acceso a los sistemas e información del Distrito. Estas conexiones incluyen el

establecimiento de páginas de inicio en la World Wide Web y el Protocolo de transferencia de archivos.

q. Colocar información del Distrito de naturaleza confidencial, sensible o patentada en Internet.

r. Duplicar ilegalmente software o su documentación relacionada.

s. Acceder a información que no sea la información que el estudiante colocó personalmente en un recurso electrónico, o que está disponible públicamente, o que el estudiante tiene autorización para acceder.

t. Cualquier actividad prohibida por la ley federal o estatal.

F. Reglas de Internet

1. La red del Distrito, incluida su (s) conexión (es) a Internet, se utilizará con fines relacionados con la educación. Cualquier uso no autorizado de Internet está estrictamente prohibido. El uso no autorizado incluye, pero no se limita a: conectar, publicar o descargar material pornográfico; participar en "piratería informática" y otras actividades relacionadas; intentar deshabilitar o comprometer la seguridad de la información contenida en las computadoras del Distrito; o el uso indebido de las computadoras del Distrito con fines ilegales o para cualquier propósito prohibido como se establece en esta política como base para la disciplina.

2. Los mensajes de Internet deben tratarse como no confidenciales. Todo lo que se envía a través de Internet pasa por varios sistemas informáticos diferentes, todos con diferentes niveles de seguridad. La confidencialidad de los mensajes puede verse comprometida en cualquier momento del camino.

3. Debido a que las publicaciones colocadas en Internet pueden mostrar el nombre y / o la dirección del Distrito, los usuarios deben asegurarse antes de publicar información en Internet que la información refleje y sea consistente con los estándares y políticas del Distrito. Antes de publicar material en línea que esté afiliado al Distrito o una organización del Distrito, incluida la creación de una cuenta de red social o página web, se requiere la autorización previa por escrito del Superintendente.

4. Es posible que se permitan las suscripciones a grupos de noticias y listas de correo cuando la suscripción sea para un propósito relacionado con la educación. Cualquier otra suscripción está prohibida.

5. La información publicada o vista en Internet puede constituir material publicado. Por lo tanto, la reproducción de la información publicada o disponible de otro modo en Internet se puede realizar únicamente con el permiso expreso del autor o titular de los derechos de autor.

6. A menos que se haya obtenido la aprobación previa del Gerente de Sistemas de Información, los usuarios no pueden establecer conexiones de Internet u otras conexiones de red externas que podrían permitir que personas no autorizadas

obtengan acceso a los sistemas e información del Distrito. Estas conexiones incluyen el establecimiento de páginas de inicio en la World Wide Web y el Protocolo de transferencia de archivos.

7. Todos los archivos descargados de Internet deben revisarse para detectar posibles virus informáticos. Si un usuario no está seguro de si su software de detección de virus está actualizado, debe consultar con el Administrador de sistemas de información antes de descargarlo.

8. Está prohibido descargar, enviar o transferir materiales ofensivos, degradantes o perjudiciales a través de Internet. Esto incluye, pero no se limita a, materiales que son inconsistentes con las políticas del Distrito con respecto a la igualdad de oportunidades educativas, el acoso sexual o cualquier ley relacionada con el acoso o la discriminación.

9. En ningún caso se colocará en Internet información de carácter confidencial, sensible o de propiedad exclusiva.

G. Notificación de anomalías o uso indebido

1. Se requiere que todos los usuarios informen cualquier anomalía o violación de seguridad tan pronto como la observen o tengan posesión de la información que ha ocurrido. Las anomalías o violaciones de seguridad se informarán al Gerente de Sistemas de Información o al Superintendente de inmediato. Los usuarios también deben reportar cualquier mal uso de los sistemas informáticos del Distrito. Si algún estudiante observa un uso indebido, como una comunicación electrónica que contiene lenguaje obsceno o acosador, el estudiante debe informar de inmediato el uso indebido al Gerente de Sistemas de Información o al Superintendente. Los estudiantes no deben mostrar el mal uso o material ofensivo ni discutir estos asuntos con nadie que no sea el Gerente de Sistemas de Información o el Superintendente.

H. Falta de privacidad y monitoreo

1. El Gerente de Sistemas de Información tendrá la discreción de monitorear aleatoriamente cualquier información registrada o almacenada por los estudiantes en los sistemas informáticos del Distrito con la aprobación del Superintendente o su designado. El Gerente de Sistemas de Información puede recuperar y revisar aleatoriamente todas las comunicaciones y los datos almacenados electrónicamente en los recursos electrónicos del Distrito, ya sean datos personales, información educativa o información relacionada con los negocios del Distrito, para asegurar que la propiedad del Distrito no esté siendo mal utilizada. Toda la información almacenada o registrada en las computadoras del Distrito u otros recursos electrónicos se considerará propiedad del Distrito.

2. Todos los estudiantes deben saber que hay información disponible sobre sus actividades informáticas. Las actividades de computación de los estudiantes no son privadas. Por ejemplo, cada vez que un estudiante accede a un sitio web en Internet, la computadora y el equipo de redes involucrados crean un rastro, descargan y muestran los archivos de Internet y, por lo general, almacenan una copia de esos

archivos en el disco duro. La computadora o servidor que mantiene la conexión a Internet también realiza un seguimiento de qué computadora ha visitado cada sitio web específico. El Distrito es propietario de las terminales de computadora, los servicios, las redes y el equipo y tiene el derecho de monitorear las actividades de los estudiantes en Internet al azar.

3. Si un estudiante reporta sospecha de mal uso de los sistemas informáticos u otros recursos electrónicos al Gerente de Sistemas de Información o al Superintendente. Al recibir dicho informe, si el Superintendente cree razonablemente, a su sola discreción, que un estudiante está haciendo un mal uso de los sistemas informáticos del Distrito u otro recurso electrónico, el Superintendente puede indicarle a un empleado designado del Distrito que revise el uso de Internet del estudiante sospechoso, u otro uso registrado electrónicamente de los sistemas informáticos o recursos electrónicos del Distrito. A su discreción, el Superintendente también puede reportar sospechas de mala conducta a los oficiales de la ley y permitir que esos oficiales accedan al uso de Internet del estudiante u otro uso registrado electrónicamente de los sistemas informáticos o recursos electrónicos del Distrito.

4. El Distrito no es responsable de ningún daño a un estudiante o cualquier otra persona causada por terceros que puedan acceder a la información personal que el estudiante ha almacenado o registrado en los recursos electrónicos del Distrito.

I. Cuestiones de derechos de autor

1. El Distrito compra y otorga licencias para el uso de varios programas informáticos para fines comerciales y no posee los derechos de autor de este software o su documentación relacionada. A menos que lo autorice el desarrollador del software, el Distrito no tiene el derecho de reproducir dicho software para usarlo en más de una computadora.

2. Los estudiantes solo pueden usar software en las redes del Distrito o en múltiples máquinas de acuerdo con el acuerdo de software aplicable. El Distrito prohíbe la duplicación ilegal de software o su documentación relacionada por parte de los estudiantes o de cualquier otra persona.

J. Vandalismo

1. El vandalismo se define como cualquier intento malicioso de alterar, dañar o destruir equipos, datos u otra propiedad del Distrito u otro usuario, o las redes conectadas a las redes del Distrito a través de Internet. Esto incluye, entre otros, la carga o creación de virus informáticos, la alteración inadecuada de datos o el uso inadecuado de información restringida. Cualquier vandalismo de los sistemas informáticos del Distrito u otros recursos electrónicos resultará en una acción disciplinaria, hasta e incluyendo la expulsión y, si corresponde, la remisión a los funcionarios encargados de hacer cumplir la ley.

K. Consecuencias por Violar esta Política

Las consecuencias por violar esta política incluyen, pero no se limitan a, una o más de las siguientes:

1. Acción disciplinaria hasta e incluyendo la expulsión;

2. Remisión a autoridades legales para enjuiciamiento bajo la sección 502 del Código Penal de California (acceso no autorizado a computadoras, sistemas y datos informáticos) u otras violaciones de las leyes estatales o federales.

3. Remisión a autoridades legales para enjuiciamiento bajo cualquier ley estatal o federal aplicable.

L. El distrito no es responsable por daños al producto del trabajo del estudiante

De vez en cuando, los sistemas informáticos del distrito fallarán o requerirán reparación o mantenimiento. El Distrito no es responsable por la pérdida o daño del producto de trabajo del estudiante causado por fallas del sistema, fallas del servidor o el desempeño del Distrito de funciones de monitoreo, mantenimiento o reparación relacionadas con sus sistemas informáticos u otros recursos electrónicos.

Referencia legal:
Código de Educación, secciones 35160 y 35160.1
Código Penal, sección 313,
18 USC, sección 1460,
18 USC, sección 2246,
18 USC, secciones 2252,
47 USC, secciones 1731 y siguientes, (Neighborhood Children's Internet Protection Act)
Nueva York v. Ferber (1982) 458 EE. UU. 747
Miller v. California (1973) 413 US 15

Fecha de la Política adoptada por la Junta: 9 de octubre de 2003
Fecha de la Política enmendada por la Junta: 12 de febrero de 2019