

PALERMO UNION SCHOOL DISTRICT

POLÍZA DE USO ACEPTABLE DE LA TECNOLOGÍA PARA LOS ESTUDIANTES

PROPÓSITO

Esta póliza proporciona los procedimientos, reglas, directrices y códigos de conducta para el uso de las redes de información y tecnología en el Distrito Escolar Unión de Palermo (PUSD). Uso de esta tecnología es un elemento necesario, natural de la misión educativa de PUSD, pero tecnología se suministra al personal y estudiantes como un privilegio, no un derecho. PUSD busca proteger, animar y mejorar los usos legítimos de la tecnología colocando justos limitaciones en su uso y sanciones para aquellos que abusan del privilegio. La reducción del abuso de la computadora proporciona recursos adecuados para usuarios con necesidades legítimas.

RESUMEN

Tecnología pública que incluye pero no limitado a computadoras, acceso inalámbrico y acceso a la red, correo electrónico, acceso a Internet, sistemas de correo de voz teléfono, dispositivos de impresión y todas las demás formas de instrucción, herramientas de red y comunicaciones se ofrecen como un servicio a los estudiantes de PUSD. Uso de estas tecnologías es un privilegio, no un derecho. Los estudiantes deben observar lo siguiente:

- Todos los usuarios están obligados a ser ciudadanos de buena tecnología por abstenerse de actividades que molestan a otros, alterar las experiencias educativas de sus compañeros, o puede ser considerado como ilegal, inmoral o conducta poco profesional.

El estudiante es responsable de sus acciones en el acceso a tecnología de PUSD. No cumplir con las directrices de uso de la tecnología puede resultar en la pérdida de privilegios de acceso o medidas disciplinarias apropiadas. Graves violaciones pueden resultar en acción civil o criminal bajo los estatutos de California o la Ley Federal.

DIRECTRICES

1. Redes de acceso a computadoras, sistemas informáticos, la información y al entorno tecnológico en el sistema de PUSD es un privilegio y debe tratarse como tal por todos los estudiantes.
2. El sistema PUSD se utilizará únicamente con el propósito de investigación, educación y relacionado con la escuela de negocios y operaciones.
3. Cualquier sistema que requiere clave de acceso o que PUSD requiere una cuenta, como Internet, será utilizado por el usuario autorizado. Los dueños de la cuenta son responsables de toda la actividad bajo su cuenta y deben cumplir con esta póliza.
4. Los recursos tecnológicos del Distrito son limitados. Todos los usuarios deben respetar el uso compartido de los recursos de PUSD. El Distrito se reserva el derecho de limitar el uso de tales recursos si no hay fondos suficientes, cuentas, almacenamiento, memoria, o por otras razones consideradas necesarias por los operadores del sistema, o si un usuario individual está determinado a actuar de manera irresponsable o manera ilegal.
5. Toda comunicación e información accesible y accedida a través del sistema PUSD es y seguirá siendo propiedad del Distrito.
6. Estudiantes deberán ser supervisado y controlado por los operadores del sistema y autorización personal. Estudiantes deben estar relacionados con el currículo de estudios.
7. Cualquier defecto o conocimiento de sospecha de abuso en sistemas PUSD, redes, seguridad, hardware o software debe ser reportado a las operaciones del sistema.

USO INACEPTABLE

El Distrito Escolar Unión de Palermo (PUSD) tiene derecho a tomar acción disciplinaria, eliminar Computadoras y redes de privilegios, o tomar acción legal o informe a las autoridades competentes, cualquier actividad que se caracteriza por ser inmoral, inaceptable o ilegal. Actividades de uso inaceptable constituyen, pero no se limitan a, cualquier actividad a través de la cual cualquier usuario:

1. Violar asuntos tales como derechos de autor institucionales o de terceros, acuerdos de licencia u otros contratos. El uso no autorizado de y/o copia del software es ilegal.
2. Interfiere o interrumpe a otros usuarios de la red, servicios o equipo. Interrupción incluyen, pero no se limitan a, distribución de publicidad, propagación de virus o gusanos no solicitados, distribución de cantidades de información que agobian el sistema (cadenas de cartas, juegos en red, etc.) o usando la red a hacer el ingreso no autorizado a cualquier otro recurso accesible a través de la red.
3. Intenta desactivar, eludir o burlar de lo contrario el PUSD el filtro de contenido que se ha instalado con arreglo a ley de Protección de los Niños/a Federal Internet. Esto incluye pero no se limita al uso de servidores proxy.
4. Trata de ganar o gana acceso no autorizado a recursos de información, obtiene copias de, o modifica archivos u otros datos, o ganancias y se comunica contraseñas pertenecientes a otros usuarios.
5. Usa o permite que otro use cualquier computadora, red informática, sistema, programa o software para diseñar o ejecutar un esquema para defraudar u obtener dinero, bienes, servicios u otras cosas de valor por pretensiones falsas, promesas, a sabiendas o representaciones.
6. Destruye, altera, desmonta, desfigura, impide el acceso legítimo a u otra forma interfiera con la integridad de los recursos de información basados en computadoras, ya sea en ordenadores independientes o en red.
7. invade la privacidad de las personas o entidades.
8. Utiliza la red para actividades comerciales o políticas o beneficio personal o privado.
9. Instala no autorizadas de software o material para su uso en equipos de Distrito. Esto incluye, pero no se limita a descargar música, fotos, imágenes, juegos y videos desde cualquier Internet o a través de unidades portátiles.
10. Utiliza la red para acceder a materiales inapropiados.
11. Utiliza el sistema de Distrito para poner en peligro su integridad (hacking software) o accesos, modifica, obtiene copias de o altera restringidos o confidencial los registros o archivos.
12. Envía, pública o muestra cualquier material difamatorio, inexacto, racialmente ofensivo, abusivo, obsceno, profano, sexualmente orientado o amenazante o mensajes públicos o privados.
13. Utiliza los sistemas de Distrito para ilegal, acoso, vandalismo, inapropiado u obsceno, o en apoyo de tales actividades está prohibido. Actividades ilegales se definen como una violación de leyes locales, estatales y/o federales. Ciber-intimidación y el acoso son insultos, comentarios, chistes, insinuaciones, comentarios desagradables, dibujos animados, bromas y otra conducta verbal relativa a un individuo que: (a) tiene el propósito o efecto de irrazonablemente interferir con el trabajo de un individuo o funcionamiento de la escuela; (b) interfiere con las operaciones de la escuela; (c) tiene el propósito o el efecto de provocar estrés emocional excesiva o miedo en un individuo.

14. El vandalismo se define como cualquier intento de dañar o destruir el sistema operativo, aplicaciones de software o datos. Uso inadecuado se define como una violación de la finalidad y objetivo de la red. Actividades obscenas se define como una violación de las normas sociales generalmente aceptadas en la comunidad para el uso de un dispositivo de comunicación públicamente poseído y funcionado.

15. Violar la póliza de Uso Aceptable del Distrito.

DERECHOS Y RESPONSABILIDADES DEL DISTRITO ESCOLAR

1. supervisar todas las actividades en el sistema del Distrito.

2. Determinar si los usos específicos de la red son consistentes con esta póliza de Uso Aceptable.

3. Eliminar el acceso de un usuario a la red en cualquier momento se determina que el usuario se dedica a la actividad no autorizada o violar esta Póliza de Uso Aceptable.

4. Respetar la privacidad de los datos electrónicos del usuario individual. El Distrito será garantizar el consentimiento de los usuarios antes de acceder a sus datos, a menos que sea requerido por ley o por pólizas de PUSD.

5. Tomar medidas prudentes para desarrollar, implementar y mantener procedimientos de seguridad para asegurar la integridad del individuo y archivos PUSD. Sin embargo, no se puede garantizar información en cualquier sistema de computadora es inaccesible por otros usuarios.

6. Intento de acceso confiable y libre de errores a los recursos de la tecnología asociados con el sistema de Distrito. Sin embargo, el distrito no se hace responsable por cualquier información que puede ser perdido, dañado, o no disponible debido a dificultades técnicas o de otras.

7. Asegúrese de que todos los usuarios de estudiante complete y firme un acuerdo para acatar la póliza de uso aceptable y regulación administrativa del Distrito. Todos esos acuerdos se mantendrán en el archivo de la oficina de la escuela.

VIOLACIONES/CONSECUENCIAS

Los estudiantes que violan esta póliza estará sujeto a revocación de acceso al sistema de PUSD hasta e incluyendo la permanente pérdida de privilegios y la disciplina hasta e incluyendo la expulsión.

Violaciones de la ley serán reportadas a las autoridades.

Acción disciplinaria puede ser apelada por los padres y estudiantes de acuerdo con los procedimientos existentes del PUSD para la suspensión o revocación de los privilegios del estudiante.

USO INACEPTABLE DE LOS SISTEMAS INFORMÁTICOS DEL DISTRITO INCLUYEN, PERO NO SE LIMITAN A, LOS SIGUIENTES:

1. Alterar cualquier configuración de computadora incluyendo protectores de pantalla, configuración de escritorio, configuración de red, contraseñas, etcétera.
2. Instalar o descargar cualquier archivo ejecutable desde Internet o unidades portátiles.
3. Uso de salas de chat o sitios web sociales excepto para fines educativos dirigidas por el maestro.
4. Instalar o utilizar programas de mensajería instantánea.
5. Descargar MP3s u otros archivos de música.
6. Acceso a programas de televisión y emisoras de radio en línea.
7. Escritura, descargar o imprimir los archivos o mensajes que contengan lenguaje inapropiado.
8. Acceder o transmitir pornografía u otro material inapropiado.
9. Violación de los derechos a la privacidad de los estudiantes y empleados del Distrito.
10. Reenvío comunicaciones personales sin el consentimiento previo del autor.
11. Copiar software comercial en violación La ley de derechos de autor.
12. Intentando hackear, agrietar, o de otra manera degradar o violar la seguridad de la red del distrito, otras redes, o computadoras individuales.
13. Intentar saltarse filtro de contenidos del distrito, incluyendo el uso de servidores proxy.
14. Desarrollar o transmitir programas que dañan un sistema informático o red, como virus.
15. Plagio.
16. Modificar o copiar archivos de otros usuarios sin su consentimiento.
17. Dar información personal como dirección y teléfono por Internet sin el permiso del personal.
18. Acceder o transmitir material que promueve la violencia o aboga por la destrucción de bienes, incluida La información relativa a la fabricación de dispositivos destructivos (explosivos, bombas, fuegos artificiales, artefactos incendiarios, etcétera).
19. Acceder o transmitir material que defiende o promueve la violencia o al odio contra determinados individuos o grupos de personas.
20. Acceder o transmitir material que defiende o promueve el uso, compra o venta de drogas ilegales.
21. Realizar o participar en cualquier actividad ilegal.
22. Cualquier acto que se determina como Acoso-cibernético, acoso o una violación de la buena ciudadanía Digital.
23. Cualquier uso inapropiado como determinado por el Superintendente, Director de tecnología y/o los administradores del edificio.