Escuelas Públicas de Olathe – Política de Uso Responsable del Personal (RUP)

I. Nuestro Compromiso con Usted y la Tecnología

A. La tecnología es una herramienta poderosa que mejora la enseñanza y el aprendizaje en las Escuelas Públicas de Olathe (el Distrito). Le proporcionamos diversas tecnologías para crear experiencias de aprendizaje atractivas e impactantes para nuestros estudiantes. Esta Política de Uso Responsable (RUP) establece nuestro entendimiento compartido sobre cómo utilizar estas tecnologías de manera efectiva y responsable.

B. Su acceso y uso de las tecnologías pertenecientes al distrito, así como de aquellas de su propiedad personal mientras se encuentra en la propiedad del distrito, en actividades relacionadas con la escuela o al utilizar la red del distrito, es un privilegio valioso que se le otorga para apoyar sus responsabilidades profesionales. Confiamos en que utilizará estos recursos de una manera alineada con nuestra misión educativa y los estándares profesionales.

C. Definición de "Tecnología":

Para los efectos de esta RUP, "tecnología" incluye:

1. La red del distrito (tanto cableada como inalámbrica)
2. Servidores
3. Estaciones de trabajo informáticas
4. Computadoras portátiles
5. Dispositivos móviles
6. Dispositivos periféricos (como ratones y teclados)
7. Bases de datos de aplicaciones
8. Recursos en línea
9. Acceso a Internet
10. Correo electrónico

11. Inteligencia artificial (IA)

12. Cualquier otra tecnología proporcionada o designada por el distrito para el uso del personal y los estudiantes, incluyendo nuevas tecnologías a medida que sean adoptadas.

D. Esta RUP se aplica siempre que usted utilice tecnologías del Distrito:

1. En la propiedad escolar o cerca de ella

2. En vehículos escolares

3. En eventos y actividades patrocinados por la escuela

4. Utilizando tecnologías y recursos propiedad del distrito fuera del campus

Nuestro objetivo al proveer estas tecnologías es apoyar su labor profesional.

II. Escuelas Públicas de Olathe: Nuestras responsabilidades

A. El distrito está comprometido a apoyarlo en el uso efectivo de la tecnología. Nuestras responsabilidades incluyen:

1. Ayudarle a desarrollar las habilidades necesarias para utilizar con éxito las tecnologías instruccionales y digitales en el ámbito laboral.

2. Proporcionar orientación y recursos para comprender el uso adecuado y responsable de las tecnologías.

3. Apoyar la integración de la tecnología en el plan de estudios y en las actividades educativas aprobadas por el distrito.

4. Facilitar el uso de tecnologías instruccionales dentro del plan de estudios y las actividades educativas aprobadas por el distrito.

B. Para garantizar la seguridad de la información del distrito, incluidos archivos confidenciales, correos electrónicos, expedientes de personal y otros datos sensibles, el distrito puede verse en la necesidad de restringir el acceso a determinadas tecnologías.

C. Tenga en cuenta que el distrito se reserva el derecho de acceder a archivos digitales, mensajes e información de cuentas del personal en cualquier tecnología o red que sea propiedad del distrito.

D. En cumplimiento con la Ley de Protección Infantil en Internet (CIPA), el Distrito capacita tanto al personal como a los estudiantes sobre el comportamiento seguro y apropiado en línea, incluyendo el uso del correo electrónico y recursos Web 2.0 (como redes sociales). También empleamos tecnologías de filtrado y medidas de seguridad para bloquear el acceso a contenido inapropiado que sea ilegal, dañino o potencialmente ofensivo. Si bien nos esforzamos por crear un entorno en línea seguro, es importante entender que no siempre es posible prevenir completamente el acceso a todo contenido inapropiado.

E. En última instancia, es responsabilidad de cada miembro del personal cumplir con las directrices sobre el uso apropiado, responsable y aceptable. Cuando el uso de la tecnología no se ajuste a estas expectativas, el distrito abordará la situación de manera adecuada.

III. Sus derechos y responsabilidades como personal

A. El uso de la tecnología es un privilegio valioso destinado para respaldar su labor profesional en las Escuelas Públicas de Olathe. Para garantizar que todos podamos beneficiarnos de estos recursos, por favor cumpla con este RUP y todas las políticas relevantes de la Junta de Educación relacionadas con el uso de la tecnología. En todas sus interacciones con la tecnología proporcionada o accesada a través del Distrito, sus derechos y responsabilidades incluyen:

1. **Respetar la privacidad**: Respete siempre los derechos de privacidad de los estudiantes y del resto del personal del distrito.

2. **Representar al distrito profesionalmente**: Comprenda que todas sus comunicaciones mediante tecnologías del distrito reflejan la integridad, ética y buen nombre del Distrito.

3. **Practicar una conducta ética**: Mantenga normas de comportamiento, conducta y cortesía éticas y aceptables, consistentes con las expectativas en nuestras escuelas y entornos del distrito.

4. **Cumplir con leyes y políticas**: Acate todas las leyes locales, estatales y federales, así como las políticas de la Junta de Educación y las directrices administrativas y escolares, especialmente aquellas relacionadas con materiales protegidos por derechos de autor.

5. **Evitar el acceso no autorizado**: No intente ni permita el acceso no autorizado a redes, tecnologías o archivos digitales de la escuela, distrito, o de entidades públicas o privadas, por ningún motivo.
6. **Seguir los procedimientos**: Cumpla con todas las políticas relacionadas de la Junta de Educación, directrices administrativas, la Matriz de Líneas de Comunicación y los procedimientos operativos escolares sobre el uso aceptable y responsable.
7. **Cooperar con investigaciones**: Coopere plenamente con los administradores del edificio y del distrito si se reporta o sospecha alguna instancia de uso inapropiado.
8. **Utilizar correctamente las tecnologías del distrito**: Utilice las tecnologías proporcionadas por el distrito (conforme a lo definido anteriormente) de acuerdo con todas las políticas y reglamentos del distrito, bajo las pautas de regulaciones federales actuales y futuras de privacidad y protección.

IV. Guía para el uso de tecnologías del distrito

A. Al utilizar las tecnologías dentro del Distrito, por favor:

1. **Practique la buena ciudadanía digital**: Siga normas adecuadas de etiqueta en línea y conducta digital responsable.

2. **Acceso a sus propios archivos**: Solo acceda, abra, visualice, modifique y/o elimine sus archivos digitales personales, trabajos educativos, cuentas de correo electrónico y contraseñas propios.

3. **Uso profesional del correo electrónico**: Utilice su cuenta de correo electrónico del Distrito únicamente para comunicaciones profesionales.

4. **Gestión del uso de banda ancha**: Limite el uso de Internet y del ancho de banda a actividades que respalden sus responsabilidades profesionales.

5. **Reporte inmediato de preocupaciones**: Informe de inmediato a un administrador o supervisor cualquier mensaje amenazante o uso/acceso inapropiado a archivos o contenidos en Internet.
6. **Comunicación respetuosa**: Utilice todas las tecnologías del distrito para comunicarse y colaborar con otros de manera amable y respetuosa.
7. **Actúe ética y responsablemente**: Asuma plena responsabilidad por sus acciones y compórtese de manera ética, incluso cuando la tecnología le brinde libertad de actuar de otra manera.

8. **Uso de acceso inalámbrico aprobado**: Utilice únicamente la red inalámbrica proporcionada por el distrito para el personal y no intente crear puntos de acceso no autorizados, como VPN personales, a ninguna tecnología perteneciente al distrito.

B. Uso responsable de la Inteligencia Artificial (IA)

1. **Intervención humana**: Mantenga la supervisión y el juicio crítico humanos al utilizar IA con estudiantes. Use la IA como compañera de enseñanza y socia intelectual, en lugar de un sustituto directo de su experiencia.
2. **Garantice la privacidad de los datos**: Mantenga la confidencialidad y seguridad de la información de estudiantes, familias y empleados, prohibiendo estrictamente la introducción de cualquier información personal identificable (PII) en herramientas o plataformas de IA.
3. **Conciencia de prejuicios**: Tenga presente que la IA puede amplificar prejuicios sociales. Fomente la evaluación crítica y analice los resultados de la IA para detectar prejuicios sociales antes de compartirlos con los estudiantes.
4. **Acceso equitativo:** Asegúrese de que todos tengan acceso, independientemente de su origen o capacidad. Al diseñar instrucción que pueda requerir el uso de IA u otras tecnologías, el personal deberá utilizar herramientas aprobadas y/o adquiridas por el distrito para las tareas estudiantiles.
5. **Comprenda la IA**: Desarrolle una comprensión crítica de las capacidades y limitaciones de las herramientas de IA antes y durante su uso con estudiantes y reflexione sobre su impacto en el aprendizaje.

V. Usos inaceptables e inapropiados de la tecnología

A. Las siguientes acciones se consideran ejemplos de usos inaceptables e inapropiados de la tecnología y serán tratadas como violaciones de la política

de la Junta de Educación y de las directrices administrativas. Las violaciones pueden conllevar medidas disciplinarias, incluida la pérdida temporal o permanente del acceso a la tecnología.

1. **No reportar uso indebido**: No reportar cualquier uso indebido o violación de la tecnología de la información al director de Tecnología de OPS o a su designado.

2. **Uso Indebido de Información Confidencial**: Obtener información confidencial sobre un estudiante o empleado para actividades no relacionadas con la escuela o compartir dicha información con fines ajenos al ámbito escolar.

3. **Acceso No Autorizado a Datos de Estudiantes**: Acceder u obtener información educativa de estudiantes sin un interés educativo legítimo.

4. **Código Malicioso**: Crear, copiar, distribuir intencionadamente o publicar cualquier tipo de software malicioso (programa maligno) en tecnologías propiedad del distrito.

5. **Suplantación y Divulgación No Autorizada**: Enviar o publicar mensajes digitales (correo electrónico, redes sociales, etc.) usando el nombre de otra persona o compartiendo información personal de otro individuo sin su consentimiento.

6. **Violaciones de Políticas en la Comunicación**: Enviar mensajes que no estén en conformidad con las políticas de la Junta de Educación o las directrices administrativas.

7. **Contenido Discriminatorio o Dañino**: Enviar mensajes con contenido sexista, racista, discriminatorio, inflamatorio o perjudicial.

8. **Mensajes Inapropiados**: Enviar mensajes inapropiados por medio de cualquier tecnología digital.

9. **Contenido Obsceno o Inapropiado**: Enviar mensajes, descargar archivos o acceder a sitios web que, a sabiendas, contengan lenguaje obsceno, gráficos,

imágenes o cualquier otro contenido inapropiado, incluyendo cualquier elemento codificado/encriptado o adjunto a mensajes.

10. **Chat en Línea No Profesional**: Participar en sesiones de chat en línea que no estén directamente relacionadas con responsabilidades profesionales.

11. **Compartir Cuentas**: Prestar su ID de cuenta o contraseña a cualquier persona.
12. **Identidad Falsa en Línea**: Crear cualquier sitio o presencia en redes sociales haciéndose pasar por otro miembro del personal.

13. **Acoso e intimidación**: Uso de lenguaje obsceno, acosador, intimidatorio o abusivo en cualquier formato digital o no digital.
14. **Medios manipulativos**: Grabar o distribuir material en línea con la intención de manipular o avergonzar a otros (personal o estudiantes).

15. **Elusión de la seguridad**: Desactivar o intentar desactivar cualquier sistema de filtrado, monitoreo o seguridad del distrito en cualquier tecnología perteneciente al distrito.

16. **Infracción de derechos de autor**: Violar las leyes de derechos de autor.

17. **Acceso no autorizado a la administración de la red**: Intentar iniciar sesión en cualquier red del distrito (alámbrica o inalámbrica) como administrador de red sin la debida autorización.

18. **Vandalismo de datos:** Dañar o destruir datos pertenecientes a otro usuario (estudiante o miembro del personal).

19. **Plagio:** Presentar el trabajo de otros como propio en tareas escolares digitales o no digitales.

20. **Violaciones generales de políticas**: Utilizar las tecnologías de cualquier manera que viole las reglas escolares, directrices administrativas, políticas de la Junta de Educación de las Escuelas Públicas de Olathe, o cualquier ley local, estatal o federal.

21. **Redes inalámbricas no autorizadas**: Acceder a redes inalámbricas que no sean de OPS con computadoras portátiles emitidas por el distrito mientras se está en el campus (incluyendo hotspots personales).

22**. Dispositivos no autorizados en la red**: Intentar conectar dispositivos no autorizados, incluidos laptops personales, teléfonos o tabletas, a la red alámbrica o inalámbrica de OPS.

23**. Comunicaciones de emergencia/traslado de teléfonos (Cumplimiento de E911):** Para cumplir con las regulaciones federales de E911 (Ley Ray Baum), que exigen información de ubicación precisa para servicios de emergencia, ningún teléfono o dispositivo de comunicación propiedad del distrito deberá ser trasladado sin la aprobación y asistencia previa de la División de Tecnología de las Escuelas Públicas de Olathe.

24**. Gestión de activos tecnológicos del distrito**: Para una gestión, seguridad y soporte efectivos, cualquier reubicación de tecnología propiedad del distrito, como computadoras, impresoras, teléfonos y otros equipos, requiere previa aprobación y coordinación con la División de Tecnología de las Escuelas Públicas de Olathe.

VI. Consecuencias del uso inaceptable e inapropiado

A. Los empleados que infrinjan esta Política de Uso Responsable (RUP), las directrices administrativas relacionadas o las políticas de la Junta de Educación de las Escuelas Públicas de Olathe respecto al Uso Responsable de Tecnologías por parte del personal, estarán sujetos a medidas disciplinarias apropiadas, que pueden incluir la terminación inmediata del empleo.

VII. Mejores Prácticas para el Uso de Dispositivos Asignados por el Distrito

A. Le animamos a ayudar a los estudiantes a interactuar activamente con la tecnología para procesar nueva información y demostrar su aprendizaje. Para apoyar este objetivo, por favor recuerde:

1. **Traiga su dispositivo**: Lleve regularmente a la escuela el(los) dispositivo(s) asignado(s) por el distrito.

2. **Use software adecuado**: Evite utilizar programas y servicios que puedan no ser apropiados para los objetivos de enseñanza y aprendizaje de un curso o materia específica.

3. **Proteja sus credenciales**: No comparta ni solicite nombres de usuario, PINs o contraseñas con otras personas.

4. **Gestión y respaldo de datos**: Aunque el distrito proporciona almacenamiento, recomendamos al personal realizar copias de seguridad periódicas de sus recursos profesionales e instruccionales en soluciones de almacenamiento personal según

sea necesario, entendiendo que el distrito no se responsabiliza de la seguridad ni de la accesibilidad de dicho almacenamiento personal y que **no se debe transferir Información Personal de Identificación o datos de estudiantes a almacenamiento personal.**

B. Mantenimiento de Dispositivos Asignados por el Distrito

1. **Reinicie regularmente**: Reinicie su dispositivo asignado por el distrito (por ejemplo, Surface Pro) al menos una vez por semana.

2. **Limpieza del historial de navegación**: Borre rutinariamente la caché y el historial de navegación para mejorar el rendimiento del dispositivo.

3. **Reporte reparaciones con prontitud**: Informe cualquier reparación necesaria (como pantalla rota, problemas con el trackpad, teclas faltantes, esquinas dobladas) al técnico de su edificio de manera oportuna.

C. Gestión de energía y ahorro de batería

1. Para prolongar la vida útil de la batería de su dispositivo cuando no esté conectado:

a. Cierre las aplicaciones que no esté utilizando.

b. Reduzca la luz de fondo del teclado.

c. Disminuya el brillo de la pantalla.

d. Apague el Wi-Fi si no lo necesita.

e. Apague el Bluetooth si no está en uso.

f. Reduzca el tiempo antes de que su computadora entre en modo de suspensión.

D. Transporte seguro de dispositivos emitidos por el distrito

1. Siempre cierre el teclado y el soporte trasero al transportar su dispositivo.

2. Evite dejar caer su dispositivo, especialmente cuando esté abierto.

3. Proteja su dispositivo de temperaturas extremas (calor o frío).

4. No apriete el dispositivo entre objetos pesados.

E. Qué evitar

1. **Uso personal del correo electrónico escolar**: Evite usar su dirección de correo electrónico del distrito para fines personales, como suscripciones y cupones.

2. **Cuentas secundarias**: No cree cuentas secundarias en su laptop emitida por el distrito (por ejemplo, para amigos, familiares o controles parentales).

3. **Sistemas operativos no autorizados**: No instale sistemas operativos distintos a los instalados por el Departamento de Tecnología de OPS (por ejemplo, Linux, máquinas virtuales).

4. **Software de intercambio de archivos no autorizado**: Evite instalar o utilizar software de intercambio de archivos de terceros sin autorización (por ejemplo, Dropbox, Torch, BitTorrent, Transmission).

5. **Uso de dispositivos personales en su lugar**: Por favor, utilice su dispositivo emitido por el distrito como su equipo principal de trabajo.

6. **Congestión de la red**: Evite enviar cadenas de correos electrónicos, mensajes de difusión inapropiados o cualquier otra información que pueda sobrecargar la red.

7. **Uso comercial**: Las tecnologías del distrito no deben utilizarse con fines comerciales. El distrito escolar no se hace responsable de ninguna obligación financiera resultante del uso de dispositivos, tecnología o acceso a internet proporcionados por el distrito (incluidas actividades relacionadas con criptomonedas).

8. **Software de seguridad no autorizado**: No instale firewalls, programas de anonimización o proxies de terceros.

VIII. Violaciones del uso responsable y aceptable: Ejemplos

Los siguientes ejemplos ilustran violaciones graves que amenazan la seguridad y protección de la red escolar, la infraestructura, los estudiantes, el personal y la comunidad en general. Estos no son exhaustivos, pero destacan áreas clave de preocupación:

A. **Privacidad, Propiedad y Comunidad**

1. Acceder o eliminar la cuenta administrativa de OPS.

2. Vandalizar o desensamblar dispositivos emitidos por el distrito u otros recursos de la red (incluyendo desfigurar, grabar, colorear, pintar, grabar con ácido, marcar, quitar teclas o deformar el dispositivo).

3. Acceder a computadoras portátiles, cuentas o archivos de otras personas sin autorización (incluyendo navegar en la computadora de otra persona, acceder a sus cuentas en línea sin su conocimiento o suplantar la identidad de alguien en línea).

4. Grabar, filmar o fotografiar a maestros, personal o estudiantes en violación de la ley, sin permiso o sin autoridad. Si se concede permiso, el material grabado debe utilizarse de manera respetuosa y responsable. No está permitido compartir ni publicar públicamente el material capturado sin un permiso adicional.

5. Utilizar dispositivos, aplicaciones o la red escolar proporcionados por el distrito (dentro o fuera de la escuela) para beneficio personal o para acosar, menospreciar o intimidar a cualquier persona o a la propia institución escolar.

6. Enviar o publicar mensajes que perjudiquen la reputación de OPS utilizando su dirección de correo electrónico escolar u otros identificadores creados por OPS.

B. **Actividad Ilegal**

1. Instalar o distribuir software no autorizado o ilegal.

2. Usar la red para apoyar actividades ilegales, negocios o juegos de apuestas. El distrito escolar no se hace responsable de ninguna obligación financiera resultante del uso de la tecnología o el acceso a internet proporcionados por la escuela en relación con dichas actividades.

C. **Violaciones de Acceso a la Red**

1. Acceder, crear o almacenar material sexualmente explícito, violento, obsceno o ilegal.

2. Intentar eludir la seguridad de la red OPS o perjudicar su funcionamiento, incluyendo el uso de VPNs o herramientas de acceso remoto (por ejemplo, GoToMyPC, LogMeIn) para evitar los protocolos de red.

3. Intentar eludir las restricciones establecidas por los administradores de red.

4. Utilizar una computadora para distribuir material inapropiado o ilegal (texto, audio, imágenes o video).

5. Proporcionar servicios facturables a terceros utilizando su computadora portátil o los recursos de la red de OPS.

6. Conectar enrutadores personales, puntos de acceso inalámbricos, altavoces inteligentes e impresoras a la red del distrito.

7. Crear una red cableada o inalámbrica sin la aprobación explícita del Departamento de Tecnología.