Política 6:235 – Exposición – la autorización para el uso de las computadoras y las redes electrónicas

El distrito 203 se ha comprometido a la excelencia educativa. Los estudiantes necesitan recopilar y sintetizar la información procedente de diversas fuentes digitales, así como también colaborar y estar en comunicación con sus compañeros y colegas de la comunidad mundial. El distrito ayudara a los estudiantes en el desarrollo de las habilidades y conocimientos necesarios para desenvolverse en el mundo que cambia rápidamente. Además, el distrito reforzará los ideales de la ciudadanía digital y lo que significa tener acceso a varios dispositivos, herramientas, redes, tecnología y poner en práctica al internet de forma responsable. Este documento hace una remisión a cualquier y todas las "computadoras", "dispositivos electrónicos", "dispositivos móviles" emitidos por el distrito, y cada uno de estos es intercambiable para los fines de esta exposición de la política.

El contenido de la exposición y los formularios de autorización están alineados con la política del distrito ***6:235, el acceso a las computadoras y a las redes electrónicas del distrito*** para promover el uso adecuado y responsable de la tecnología como apoyo de la misión y los objetivos del distrito. Además, otras políticas pertinentes del distrito desempeñan un papel en el uso exitoso de las computadoras y a las redes electrónicas del distrito, incluyendo pero no limitado a: ***6:235 AP-1*** sobre ***el uso aceptable de las computadoras y las redes electrónicas del distrito*** y ***7:180*** *para* ***prevenir el acoso, la intimidación y el tormento***. Cualquier empleado, estudiante, u otra persona que participa en una actividad que involucra el uso de los recursos electrónicos del distrito (los sistemas y/o las redes y/o las computadoras emitidas por el distrito (o las computadoras personales para el uso escolar)) debe cumplir con las políticas establecidas por la junta de educación, así como las directrices complementarias y todas las leyes federales y estatales pertinentes. Dichas leyes y políticas están sujetas a cambios sin previo aviso.

Términos y condiciones

El acceso a las redes y a los sistemas del distrito debe apoyar a la educación y/o las investigaciones, y ser coherente con las metas educativas del distrito. Los términos y condiciones de uso aceptable no intentan afirmar todo el comportamiento requerido por los estudiantes; sin embargo, algunos ejemplos concretos son proporcionados. Si un estudiante no sigue estas directrices, esto puede resultar en la pérdida de privilegios, acción disciplinaria, y/o acción legal adecuada.

El uso inaceptable

- Intentar dañar o destruir los sistemas o equipos de red del distrito, los datos.
- Intentar dañar o destruir los datos o el dispositivo de otro estudiante o el usuario de sistemas y de las redes del distrito.
- Intentar degradar o interrumpir los sistemas o las redes del distrito descargando o modificando el malware (programa malicioso) es vandalismo y puede constituir un acto delictivo bajo las leyes estatales o federales.
- Utilizando los sistemas o las redes del distrito para cualquier actividad ilegal, incluyendo la violación de los derechos de autor u otros contratos, o transmitir cualquier material en violación de cualquier ley de los EE.UU. o estatal.
- Descargar software (programas de computadoras) no autorizadas.
- Descargar o almacenar material plagiado, para uso solo de los derechos de autor o material protegido por secreto comercial.
- El uso de las redes y los sistemas del distrito para beneficio de financiación privado o comercial.

- Desperdiciar los recursos electrónicos del distrito, tales como el espacio de archivos, la impresión o el uso excesivo de banda ancha.
- Obtener acceso no autorizado a los archivos, recursos, o entidades.
- Invadiendo la privacidad de las personas, incluyendo divulgación no autorizada, difusión y utilización de la información, o publicar mensajes anónimos.
- Participar en publicaciones de blog, publicaciones de web o foros de discusión que violan las leyes estatales o federales.
- Fraudulentamente utilizando la cuenta o la contraseña de otro estudiante.
- Publicar material autorizado o creado por otro sin su consentimiento.
- Utilizando los sistemas o la red del distrito para fines comerciales o publicidad privada.
- Intencionalmente descargar malware, por cualquier motivo, incluyendo virus, troyanos, gusanos, ladrones de contraseñas, o cualquier otro producto destinado para omitir la seguridad del distrito o las directrices de uso aceptable.
- Accediendo, presentando, publicando, enviando mensajes de texto o mostrando cualquier información difamatoria, inexacta, abusiva, profana, obscena, sexualmente orientada, amenazadora, racistas, de acoso, de intimidación o actividades ilegales.
- Utilizando los sistemas o redes del distrito mientras los privilegios de acceso son suspendidos o revocados.
- Utilizando los sistemas o las redes del distrito como una puerta de enlace o punto intermediario de tránsito para cargar los datos a un dispositivo remoto, no del distrito o personal.
- Modificar o cambiar las configuraciones del sistema sin permisos adecuados.

Cualquier estudiante que plantea repetidamente un riesgo para la seguridad de los sistemas o las redes del distrito puede ser sujeto a las medidas disciplinarias de conformidad con las políticas de disciplina actuales del distrito. Además, el distrito puede adoptar medidas disciplinarias por la conducta iniciada y/o creada fuera de la escuela que involucra la utilización inadecuada del internet o recursos basados en el web, si esa conducta constituye una amenaza o interfiere considerablemente o interrumpe las operaciones y el buen orden de las escuelas del distrito e instalaciones, incluyendo hostigamiento entre alumnos y/o el acoso entre los estudiantes, independientemente de que la acción involucro el uso de los sistemas y las redes del distrito.

El uso general

No se ofrecen garantías de ningún tipo, ya sean expresadas o implícitas, para el servicio prestado por los sistemas o las redes del distrito. El distrito no será responsable por ningún daño que resulte de la pérdida de datos debido a las interrupciones del servicio causadas por su negligencia o errores u omisiones del estudiante.

La seguridad de todos los sistemas y las redes de distrito es de suma importancia y varios procesos y programas son constantemente ejecutados para vigilar e informar los riesgos de seguridad. La participación en los procesos de seguridad y los programas es obligatoria, y todos los dispositivos conectados a la red del distrito, ya sea emitido por el distrito o personales (para el uso escolar), deben someterse a los escaneos de seguridad y rejas. Los estudiantes pueden apoyar esta posición crítica de seguridad manteniendo todos nombres de usuario y contraseñas confidenciales. Si un estudiante sospecha o descubre un riesgo de seguridad, ese riesgo debe ser comunicado inmediatamente a su maestro quien notificara al equipo de servicio de asistencia técnica escolar.

La ciudadanía digital

La ciudadanía digital es el concepto de educar a todos los estudiantes en el uso adecuado de la tecnología. Un buen ciudadano digital es una persona que sabe lo que es correcto y lo incorrecto, demuestra un comportamiento tecnológico inteligente y hace buenas decisiones al usar la tecnología.

Se espera que todos los estudiantes cumplan con las normas generalmente aceptadas de etiqueta de redes y las condiciones de la buena ciudadanía digital. Esto incluye, pero no se limita a:

1. **Respetarse a sí mismo.** Seleccione nombres para uso en línea que sean adecuados, y examine la información y las imágenes publicadas en línea. Considere seriamente cualquier información personal que tenga que ver con las experiencias de la vida, la experimentación y las relaciones que publique en línea. Reconocer que el correo electrónico (e-mail), en todas sus formas, no es privado y que el distrito reserva el derecho de acceso al correo electrónico proporcionado por el distrito, así como todos los demás sistemas de datos del distrito sin previo aviso o permiso. Si se descubre mensajes o datos relativos a, o en apoyo de, actividades ilegales, estos pueden ser informados a las autoridades legales.

2. **Protegerse a sí mismo**. Asegurarse de que la información, imágenes, y los materiales publicados en línea no lo van a poner en riesgo. No publicar información personalmente identificable, como domicilios, números de teléfono, fechas de nacimiento, números de seguro social, datos de contacto, calendario de actividades personales, etc. Informe cualquier agresión o comportamiento inadecuado. Proteger las cuentas, contraseñas y recursos, y cambiar las contraseñas en cumplimiento con las políticas del distrito. No proporcione información del nombre de usuario o contraseña del distrito por correo electrónico a cualquiera por cualquier motivo. Tenga en cuenta que el distrito nunca le enviará un correo electrónico solicitando información sobre cualquier tipo de información de seguridad tal como un nombre de usuario, contraseña, etc.

3. **Respetar a los demás**. No utilizar medios electrónicos para antagonizar, acosar, atormentar, o seguir/acechar a alguien. No visite sitios que son degradantes, pornográficos, racistas, o de lo contrario inadecuados. No abuse los derechos de acceso, y no introducirse a otras áreas o espacios privados de personas. Ser educado y no ser abusivo en los mensajes a los demás. No decir maldiciones, o usar groserías, o cualquier otro tipo de lenguaje inapropiado. No utilizar los sistemas o red del distrito de cualquier manera que pueda interrumpir su uso por otras personas.

4. **Proteger a los demás**. Informar el abuso y no remitir material inadecuado o comunicaciones. Ser consciente de, y evitar materiales inaceptables y las conversaciones. No divulgue información personal identificable de los estudiantes o colegas.

5. **Respetar la propiedad intelectual**. Solicitar permiso para utilizar los recursos. Citar cualquier y todo uso de los sitios web, libros y medios de comunicación. Reconocer las fuentes principales y validar la información. Utilizar y cumplir con el uso de las reglas justas.

6. **Proteger la propiedad intelectual**. Solicitar permiso para utilizar el software y medios de comunicación que otros producen. No robar software y utilizar solo el software que el distrito ha comprado, con licencia, y ha inscrito. Actuar con integridad y reconocer que todas las comunicaciones y la información accesible a través de redes y sistemas son propiedad privada.

No hay expectativas de la privacidad de los datos

El distrito se reserva el derecho a acceder y divulgar el contenido de cualquier cuenta de cualquier sistema del distrito, incluidos los externos, tales como Gmail, sin necesidad de previo aviso o permiso del dueño de la cuenta. De esta forma, los estudiantes y el personal no tienen expectativas de confidencialidad o privacidad con respecto a cualquier comunicación o acceso a través de redes y sistemas del distrito o en las computadoras emitidas por el distrito, independientemente si la utilización es para el distrito o con fines personales, que no sean específicamente previstos por la ley. El distrito podrá, sin previo aviso ni consentimiento, registrar, supervisar, acceder, monitorear, ver o grabar el uso de sistemas y redes del distrito (incluyendo la revisión de archivos y otros materiales) en cualquier momento. Por medio del uso o acceso a la tecnología del distrito, todos los estudiantes están de acuerdo a dicho acceso, supervisión y/o la grabación de su uso.