

## **Código Política: Uso Responsable de Tecnología 3225/4312/7320**

La junta educativa le proporciona a los estudiantes y al personal acceso a una variedad de recursos tecnológicos. Estos recursos proporcionan oportunidades para mejorar el aprendizaje y mejorar la comunicación dentro de la comunidad de la escuela y para una comunidad globalmente más grande. A través de los recursos tecnológicos del sistema escolar, los usuarios pueden observar los acontecimientos a medida que ocurren en todo el mundo, interactuar con otras personas en una variedad de temas y tener acceso a información actual y profunda.

Es el propósito de la junta que los estudiantes y los empleados se beneficien de estos recursos siempre y cuando su uso esté dentro de los límites de uso seguro, legal y responsable. Por lo tanto, la Junta establece esta política para observar el uso de los recursos tecnológicos del sistema escolar por parte de los estudiantes y empleados. Esta política aplica al uso que se produzca dentro o fuera del sistema escolar, y se aplica a todos los recursos tecnológicos del sistema escolar, incluyendo pero sin limitar a las redes de ordenadores y conexiones, los recursos, las herramientas y los entornos de aprendizaje puestos a disposición por o en la redes, y todos los aparatos de tecnología que se conectan a esas redes.

### **A. Las expectativas para el uso de los recursos tecnológicos de la escuela.**

El uso de los recursos tecnológicos del sistema escolar, incluyendo el acceso a Internet, es un privilegio, no un derecho. Los usuarios individuales que usan los recursos tecnológicos del sistema escolar son responsables de su comportamiento y las comunicaciones al utilizar esos recursos. El uso responsable de los recursos tecnológicos del sistema escolar debe ser ético, respetuoso, honesto académicamente y que apoye el aprendizaje de los estudiantes. Cada usuario dispone de la exclusiva responsabilidad de respetar a los demás en la comunidad escolar y en Internet. Se espera que los usuarios cumplan con las normas generalmente y acepten las reglas de etiqueta de la red. Las normas de conducta de los estudiantes y de los empleados en general, incluyen las políticas establecidas por la junta, como el Código de Conducta de Estudiantes y otros reglamentos y normas de la escuela, se aplicaran al uso de Internet y otros recursos tecnológicos de la escuela.

Además, cualquier persona que utilice las computadoras del sistema escolar o aparatos electrónicos o que acceda a la red de la escuela o Internet a través de los recursos del sistema de la escuela debe cumplir con las reglas adicionales para el uso responsable de la sección B, a continuación. Estas normas tienen por objeto aclarar las expectativas de conducta, pero no se deben interpretar como un todo.

Antes de usar el Internet, todos los estudiantes deben estar entrenados sobre el comportamiento en línea adecuada según la política de 3226/4205, y la seguridad en el Internet.

Todos los estudiantes y los empleados deben ser informados anualmente de los requisitos de esta política y los métodos por los cuales se puede obtener una copia de esta política. Antes de utilizar los recursos tecnológicos del sistema escolar, los estudiantes y los empleados deben firmar una declaración indicando que entienden y estrictamente cumplirán con estos requisitos. El incumplimiento de estos requisitos dará lugar a una acción disciplinaria, incluyendo la revocación de los privilegios del usuario. El mal uso intencional puede resultar en una acción disciplinaria y/o el enjuiciamiento penal por las leyes estatales y federales.

### **B. Normas de uso de los recursos tecnológicos de la escuela.**

1. Los recursos tecnológicos del sistema escolar se proporcionan para el uso apropiado y legal de conformidad con la política de 3220. Los usos aceptables de tales recursos tecnológicos se concentran en las actividades responsables, eficientes y legales que apoyan el aprendizaje y la enseñanza. El uso inapropiado de los recursos tecnológicos del sistema escolar por parte de los maestros y estudiantes para la diversión o entretenimiento esta prohibido. El uso personal de los aparatos de tecnología de los empleados

y estudiantes se permite siempre y cuando que se produzca en su tiempo personal y no interfiera con la instrucción del sistema escolar, y no este prohibido por la política de la junta o procedimientos.

2. Bajo ninguna circunstancia el software adquirido por el sistema escolar se puede copiar para uso personal.

3. Los estudiantes y los empleados deben cumplir con todas las leyes, incluyendo las relacionadas a los derechos de autor y marcas comerciales, información confidenciales y los registros públicos. Cualquier uso que viole la ley estatal o federal está terminantemente prohibida. El plagio de los recursos de Internet serán tratados de la misma manera que cualquier otro incidente de plagio, como se indica en el Código de Conducta del Estudiante.

4. Ningún usuario de los recursos tecnológicos, incluyendo las personas que envían y/ o reciben comunicaciones electrónicas, pueden participar en la creación, ver, acceder, descargar, guardar, imprimir o transmitir intencionalmente imágenes, gráficos (incluyendo imágenes fijas o en movimiento), archivos de sonido, texto archivos, documentos, mensajes o cualquier otro material que sea obsceno, difamatorio, profano, pornográfico, acosador, abusivo, o que se considera perjudicial para los menores.

5 Está prohibido el uso de agentes anónimos para evadir el filtrado de contenido.

6. Los usuarios no pueden instalar o utilizar cualquier programa de intercambio de archivos en Internet diseñado para facilitar el intercambio de material con derechos de autor.

7. Los usuarios de los recursos tecnológicos no pueden enviar comunicaciones electrónicas de manera fraudulenta (es decir, al tergiversar la identidad del remitente).

8. Los usuarios deben respetar la privacidad de otros. Cuando utilicen el correo electrónico, salas de chat, blogs, u otras formas de comunicación electrónicas, los estudiantes no deben revelar información sobre la identificación personal o información que sea privada o confidencial, como el domicilio o número de teléfono, tarjeta de crédito o información de cuenta de cheques, o número de seguro social propio o de los compañeros de estudios.

Además, los empleados de la escuela no deben revelar en los sitios web del sistema escolar o páginas web o en otros lugares en Internet información relacionada a los estudiantes, privada o confidencial (incluyendo nombres, direcciones, o imágenes) sin el permiso por escrito de un padre o tutor o de un estudiante elegible, excepto lo explícito de otra manera por los Derechos Educativos de la Familia y la Ley de Privacidad (FERPA). Los usuarios tampoco pueden remitir o enviar comunicaciones personales sin el consentimiento previo del autor.

9. Los usuarios no pueden deliberadamente o por negligencia dañar computadoras, sistemas informáticos, aparatos electrónicos, software, redes informáticas, o datos de cualquier usuario conectado al sistema escolar. Los usuarios no pueden transmitir sabiendo o por negligencia virus informáticos o mensajes de auto-replicantes o deliberadamente tratar de degradar o interrumpir el desempeño del sistema.

10. Los usuarios no pueden crear o introducir programas de comunicaciones de red, o cualquier programa extranjero o software en cualquier computadora del sistema escolar, aparatos electrónicos, o de la red sin la autorización expresa del director de tecnología o la persona designada.

11. Los usuarios tienen prohibido participar en actividades que no están autorizados o ilegales, tales como "hacking" o el uso de la red informática para obtener o intentar obtener acceso no autorizado o ilegal a otros computadores, sistemas informáticos, o cuentas.

12. Los usuarios tienen prohibido el uso de identificación de otro individuo o la contraseña de cualquier recurso tecnológico.

13. Los usuarios no pueden leer, alterar, cambiar, bloquear, ejecutar o eliminar archivos o comunicaciones pertenecientes a otro usuario sin el permiso expreso previo del propietario.

14. Los empleados no deben usar contraseñas o identificadores de usuario de cualquier sistema de datos (por ejemplo, la información estatal de un estudiante y las aplicaciones de sistemas de mejora de instrucción, el software de cronometraje, etc.) para un fin no autorizado o inapropiado.

15. Si un usuario identifica un problema de seguridad en un recurso tecnológico, él o ella debe notificar inmediatamente a un administrador del sistema. Los usuarios no tienen que demostrar el problema a otros usuarios. Cualquier usuario identificado como un riesgo de seguridad se le negará el acceso.

16. Los maestros harán todo lo posible para supervisar y vigilar de cerca el uso de Internet de los estudiantes durante el tiempo de instrucción.

17. Las opiniones se pueden expresar a través de Internet o de otros recursos tecnológicos como la representación de la opinión del sistema escolar o parte del sistema de la escuela solamente con la aprobación previa del superintendente o su designado.

### **C. MATERIAL LIMITADO EN INTERNET**

El Internet y las comunicaciones electrónicas ofrecen entornos de fluidos en el cual los estudiantes pueden acceder o estar expuestos a materiales e información de diversas fuentes y en rápida evolución, incluyendo algunos que pueden ser perjudiciales para los estudiantes.

La Junta reconoce que es imposible predecir con certeza qué tipo de información los estudiantes pueden acceder u obtener en el internet.

Sin embargo el personal del sistema escolar deben tomar precauciones razonables para evitar que los estudiantes tengan acceso a material y la información que sea obsceno, pornográfico, o de otra manera perjudicial para los menores, incluyendo violencia, desnudez, o lenguaje gráfico que no sirve como propósito pedagógico legítimo.

El superintendente debe asegurarse de que en la tecnología se utilizan medidas de protección, la seguridad en Internet, y se desactivan o minimizan sólo cuando lo permita la ley y la política de la junta.

La junta no se hace responsable por el contenido accedido por los usuarios que se conectan al Internet a través de su teléfono móvil personal (por ejemplo, 3G, 4G servicio).

### **D. CONSENTIMIENTO DE LOS PADRES**

La Junta reconoce que los padres de los menores de edad son responsables de establecer y transmitir los estándares que sus hijos deben seguir cuando usan medios de comunicación y de información. Por lo tanto, antes de que un estudiante pueda acceder al Internet independientemente, el padre del estudiante debe ser consciente de la posibilidad de que el estudiante puede obtener acceso a material inapropiado mientras usa independiente el Internet. El padre y el estudiante deben de estar de acuerdo con el acceso independiente del estudiante al Internet y la supervisión del personal escolar de la comunicación del correo electrónico de los estudiantes.

Además, de acuerdo con los objetivos de la junta directiva y la visión de la tecnología, los estudiantes pueden pedir cuentas por una tercera persona para proyectos relacionados con la escuela diseñados para ayudar a

los estudiantes en el dominio de las comunicaciones efectivas en línea y adecuados o para satisfacer otras metas educativas. Se obtendrá el permiso de los padres cuando sea necesario para crear y administrar las cuentas de tales terceras personas.

## **E. PRIVACIDAD**

No existe un derecho a la privacidad en el uso de los recursos tecnológicos. Los usuarios no deben suponer que los archivos o comunicaciones creados o transmitidos usando de los recursos tecnológicos del sistema escolar o almacenados en los servicios o unidades de disco duro de las computadoras individuales serán privada. Los administradores del sistema escolar o personas designadas por el superintendente pudran revisar los archivos, monitorear todas las comunicaciones e interceptar mensajes de correo electrónico para mantener la integridad del sistema y asegurar el cumplimiento de la política del consejo y de las leyes y reglamentos pertinentes. El personal del sistema escolar controlará las actividades en línea de las personas que acceden al Internet a través de computadoras que son propiedad de la escuela.

## **F. SITIOS WEB PERSONALES**

El superintendente puede utilizar cualquier medio disponible para solicitar la eliminación de páginas web personales que alteran significativamente el ambiente escolar o que utilizan el sistema de la escuela o nombres de las escuelas, logotipos, marcas registradas o sin permiso.

### **1. Los estudiantes**

Aunque el personal de la escuela en general no controlan las actividades que los estudiantes hacen en el internet y otros aparatos de tecnología que no son del sistema escolar y que no se usan durante las horas escolares y cuando el comportamiento en línea de los estudiantes tiene un efecto directo e inmediato en la seguridad escolar o el mantenimiento del orden y la disciplina en las escuelas, el estudiante puede ser disciplinado de acuerdo con la política del consejo.

### **2. Los empleados**

Los sitios web personales de los empleados están sujetos a la política 7335, "*Employee Use of Social Media*".

### **3. Los voluntarios**

Los voluntarios deben mantener una relación adecuada con los estudiantes en todo momento.

Se les sugiere a los voluntarios que no dejen a los estudiantes ver su información personal de sus paginas o perfiles de redes en línea con el fin de evitar la posibilidad de que los estudiantes ven materiales que no son apropiados para su edad. La relación de un voluntario en particular con el sistema escolar puede ser terminada sí el voluntario participa en la interacción en línea inapropiada con los estudiantes.

Legal References: **U.S. Const. amend. I**; Children's Internet Protection Act, **47 U.S.C. 254** (h)(5);

Electronic Communications Privacy Act, **18 U.S.C. 2510-2522**; Family Educational

Rights and Privacy Act, **20 U.S.C. 1232g**; **17 U.S.C. 101 et seq.**; **20 U.S.C. 6777**; **G.S. 115C-**

**325(e)** (applicable to career status teachers), **-325.4** (applicable to non-career status teachers)

Cross References: Curriculum and Instructional Guides (policy 3115), Technology in the Educational Program (policy 3220), Internet Safety (policy 3226/4205), Copyright Compliance (policy 3230/7330), Web Page Development (policy 3227/7322), Student Behavior Policies (all policies in the 4300 series), Student Records (policy 4700), Confidentiality of Personal Identifying Information (policy 4705/7825), Public Records – Retention, Release, and Disposition (policy 5070/7350), Use of Equipment, Materials, and Supplies (policy 6520), Network Security (policy 6524), Staff Responsibilities (policy 7300), Employee Use of Social Media (policy 7335)

Adoption: 8/4/2014

