Política de Seguridad de Internet para el Distrito Escolar Unificado de Princeton

Introducción
Es la política del Distrito Escolar Unificado de Princeton de: (a) impedir el acceso de usuarios a través de su red de computadoras , o transmisión de material inapropiado a través de Internet, correo electrónico u otras formas de comunicación electrónica directa; (b) impedir el acceso no autorizado y otras actividades ilegales en la red social;(c) evitar la divulgación no autorizada en línea, usar o divulgar información personal de menores de edad; y (d) cumplir con la Ley de Protección de Niños en la Internet (Children's Internet Protection Act) [Pub. L. No. 106-554 y 47 USC 254 (h)].

Definiciones
Los términos claves son como están definidos en Children's Internet Protection Act.

Acceso a Material Inapropiado
Al mayor grado posible, medidas de protección de Tecnología (o los filtros de Internet) serán usadas para bloquear o filtrar el Internet, u otras formas de comunicaciones electrónicas, acceso a información inapropiada. Específicamente, según lo requerido por la Ley de Protección de Niños in Internet, el bloqueo se aplicará a representaciones visuales de material considerado obsceno o cualquier material considerado perjudicial para menores. Sujeto a supervisión del personal, medidas de protección de tecnología pueden ser desactivadas para adultos o, en caso de menores, minimizados sólo para investigaciones de buena fe u otros objetivos legales.

Uso Inapropiado de la Red
Al mayor grado posible, medidas serán tomadas para promover la seguridad y la seguridad de los usuarios del Distrito Escolar Unificado de Princeton de la red de computadora en línea cuando usen correo electrónico, salas de Chat, mensajería de Internet, y otras formas de comunicación electrónica directa. Específicamente, como requerido por el Children's Internet Protection Act, prevención del uso de red inadecuado incluye: (a) acceso no autorizado, incluyendo el tan - llamado "hacking", y otras actividades ilegales; y (b) divulgación no autorizada, uso, y diseminación de información de identificación personal respecto a menores.

Reportando y la Investigación de Violaciones
Usuarios de los sistemas informarán violaciones de esta política, preocupaciones de seguridad del sistema, o sospechas de actividades del sistema ilícitas o incorrectas a la administración. Inspección y vigilancia de los recursos de información puede ser necesaria para fines de hacer cumplir estas medidas, conduciendo investigaciones, lo que garantiza la seguridad o el cumplimiento de la ley. Usuarios de recursos de información deben cooperar con cualquier investigación de abuso de políticas. La falta de cooperación puede ser motivo para la cancelación de los privilegios de acceso, u otras acciones disciplinarias.

Educación, Supervisión y Monitoreo
Será responsabilidad de todos lo miembros del personal del Distrito Escolar Unificado de Princeton educar, supervisar y controlar el uso adecuado de la red de computadoras en línea y acceso a Internet de acuerdo con esta política, la ley Children's Internet Protection Act, el Neighborhood Children's Internet Protection Act, y la ley Protecting Children in the 21st Century Act. Los procedimientos para la desactivación o por otra parte modificación de cualquier medida de protección de tecnología serán la responsabilidad del Director de Información de Tecnología de la Oficina de Educación del Condado de Glenn o representantes designados.

El Superintendente del Distrito Escolar Unificado de Princeton designó representantes para proporcionar capacitación apropiada a la edad de los estudiantes que utilizan la Internet en las instalaciones del Distrito Escolar Unificado de Princeton. El entrenamiento proveído será designado para promover el compromiso del Distrito Escolar Unificado de Princeton de:

a. Las normas y uso aceptable de la Internet están establecidas en las Normas de Seguridad de Internet del Distrito Escolar Unificado de Princeton,

b. Seguridad del Estudiante con respecto a:
    i. Seguridad en el Internet;
    ii. Conducta apropiada mientras estén en línea, en redes sociales de sitios Web, y en las alas de chat, y
    iii. Conocimiento de acoso cibernético (cyber bullying) y respuesta.

c. Cumplir con los requisitos de E-rate de la ley Children's Internet Protection Act (CIPA).

Tras recibir este entrenamiento, el alumno reconocerá que el/ella recibió la capacitación, la entendió, y seguirá las disposiciones de las políticas del Distrito del uso aceptable.

Adopción
Esta política de Seguridad de Internet fue aprobada por la Mesa Directiva del Distrito Escolar Unificado de Princeton, en una reunión publica, después del aviso publico normal, el 13 de diciembre, 2012.

- **Definiciones de los términos CIPA**:

Menor. El término "menor" significa cualquier individuo que no ha cumplido 17 años de edad.

MEDIDA DE PROTECION DE TECNOLOGIA. El término "medida de protección tecnológica" significa una tecnología específica que bloquea o filtra el acceso a representaciones visuales que son:

1. **OBSCENO**, tal como está definido en la sección 1460 del titulo 18, del código de Estados Unidos;
2. **PORNOGRAFIA INFANTIL,** como está definido en sección 2256 del título 18, Código de Estados Unidos; o
3. perjudicial a otros.

PERJUDICIAL PARA LOS MENORES. El término "perjudicial para menores" significa cualquier foto, imagen, archivos de imagen grafica, u otra representación visual que:

1. Tomado en conjunto y con respecto a menores, peticiones a un interés lascivo a desnudez, sexo o excreción;
2. Representa, describe o muestra en forma patentemente ofensiva con respecto a lo que es apropiado para menores, un contacto sexual real o simulado, verdaderos o simulados actos sexuales normales o pervertidos, o una exhibición lasciva de los genitales; y
3. En conjunto, carece de serio valor literario, artístico, político o valor científico paro los menores.

ACTO SEXUAL; CONTACTO SEXUAL. Los términos "acto sexual" y "contacto sexual" tienen los términos de los significados en la sección 2246 del titulo 18, del código de Estados Unidos.

Distrito Escolar Unificado de Princeton
Entrenamiento de Seguridad de Internet

A fin de proteger a nuestros estudiantes, garantizar el uso apropiado de red/Internet, y calidad para la financiación federal de las telecomunicaciones E-Rate, los profesores de Princeton proporcionarán instrucción sobre la red apropiada y el uso de Internet a los estudiantes de Princeton. El plan de estudios es de commonsensemedia org. Un proveedor federal E-Rate recomendado. Las lecciones son para el uso apropiado a la edad.

Grado	Tema
K	**Ir a Lugares Con Seguridad**: Estudiantes aprenden a que ellos pueden ir a interesantes sitios en línea, pero ellos tienen que seguir ciertas reglas para permanecer a salvo.
1	**Envío de Correo Electrónico**: Estudiantes exploran como ellos pueden utilizar correos electrónicos para comunicarse con personas reales dentro de su escuela, familias y comunidad.
2	**Mostrar Respeto en la Red**: Estudiantes exploran lo que significa acoso cibernético y lo que pueden hacer cuando lo encuentran. Estudiantes aprende sobre las comunicaciones en persona y en línea, y como escribir emails buenos.
3	**Conversando de Forma Segura en Línea:** los estudiantes aprenden que el Internet es un gran lugar para desarrollar relaciones provechosas. Pero ellos también aprenden a no revelar información privada a una persona que ellos conocen sólo en línea.
4	**El Poder de Palabras**: Los estudiantes consideran que pueden recibir mensajes en la Internet de otros estudiantes que pueden hacerlos sentirse enojados, heridos, tristes, o con temor, Ellos exploran maneras para manejar el acoso cibernético si eso sucede.
5.	**Promesa de Ciudadanía Digital:** los Estudiantes trabajan juntos para perfilar expectativas comunes a fin de construir una comunidad fuerte de ciudadanía digital. Cada miembro de la clase firma un Nosotros Promesa Ciudadana Digita**l.**
6.	**Conversación en la Red sin Peligro:** los Estudiantes consideran escenarios en los cuales ellos podrían sentirse incómodos o encontrar conversación o comportamiento inadecuado en línea. Ellos aprenden a reconocer a depredadores en línea y reglas para la seguridad en línea.
6	**Fraudes y Esquemas:** los Estudiantes aprenden estrategias para protegerse contra robo de identidad y estafadores que tratan de tener acceso a su información privada en línea**.**
7	**Acoso Cibernético: Cruzando la Línea**: Los Estudiantes aprenden a distinguir bromas bondadosas a las de acoso cibernético.
7	**Huella de un Trillón de Dólares**: Los estudiantes aprenden que tienen una huella digital y que ésta información se puede buscar; copiar y transmitir, pero ellos pueden tener un tipo de control basado en lo que ellos publiquen en la Red.
8	**¿Cuál Yo deberé ser?** Los estudiantes aprenden que presentarse a si mismos de modos diferentes en la Red lleva tanto beneficios como riesgos.
8	**Cyberbullying: Sé Honrado**: Los estudiantes aprenden acerca de la diferencia entre ser un espectador pasivo versus un espectador valiente en situaciones de acoso cibernético.
9	**Privado Hoy, Publico Mañana**: Los estudiantes reflexionan sobre su responsabilidad de proteger la privacidad de otros cuando publican información sobre ellos en la Red.
10	**Relaciones Peligrosas en la Red**: Los estudiantes piensan críticamente sobre el desarrollo de relaciones con personas en la Red.
11	**Collage Bound**: Los estudiantes aprenden que todo lo que ellos o alguien más publican sobre ellos en la Red se convierte en parte de la presencia pública en la Red conocida como una huella digital.
12	**Tomando Perspectivas Sobre el Acoso Cibernético:** Los estudiantes aprenden respecto a la dinámica de la crueldad en la Red y como afecta a todas las personas involucradas.

Todas las lecciones disponibles en: http://www.commonsensemedia.org/educators/erate-teachers