(SPANISH (LATIN AMERICAN))

Regulación 295-1
ADMINISTRACIÓN ESCOLAR GENERAL
1 de julio de 2012

ADMINISTRACIÓN ESCOLAR GENERAL

Sistemas de computación y servicios de redes. Política de seguridad de Internet y uso aceptable de las PWCS

Esta regulación contiene la Política de Seguridad de Internet y uso aceptable de las Escuelas Públicas del Condado de Prince William, conforme lo autorizado en la Política 295, Normativa para el uso de tecnología de telecomunicaciones e Internet. Esto regula el uso de todas las redes locales del área de las Escuelas Públicas del Condado de Prince William (PWCS), con cables e inalámbricas, redes de área ancha, los sistemas relacionados con Internet, intranet y extranet, todos los sitios web de las PWCS y todas las otras redes similares. Esta política también aplica específicamente al uso del equipo de computación de las PWCS; software; sistemas operativos; medios de almacenamiento; cuentas de redes que proporcionan acceso a servicios de red, tales como el correo electrónico; navegación en la web y sistemas de archivo; así como tecnologías de telecomunicaciones tales como los teléfonos, las computadoras personales, los teléfonos celulares, los Asistentes Digitales Personales (PDA), las máquinas de facsímil y todos los otros aparatos de telecomunicación con cable o inalámbrica.

Está limitado el uso de los aparatos personales de los estudiantes o del personal en las escuelas y las clases y deben cumplir con esta regulación y con todas las otras políticas y regulaciones de la Junta Escolar. Se permiten los sistemas de computación que no sean propiedad de las PWCS o de uso personal, para conectarse únicamente a la red inalámbrica de visitantes de las PWCS y no pueden conectarse de ninguna otra manera a ninguna otra propiedad o red de las PWCS. Además, para asegurar el cumplimiento con las leyes federales y estatales correspondientes, los lineamientos y las regulaciones del Departamento de Educación de Virginia, y las políticas y regulaciones de la Junta Escolar, los sistemas de computación que no sean de las PWCS no pueden ser utilizados para la enseñanza o para negocios oficiales de las PWCS a menos que sea haya aprobado explícitamente por el Directorio de Servicios de Tecnología de la Información o su representante.

Hasta donde esta regulación pueda aplicar a otras tecnologías de la información y de telecomunicación, se interpretará como que aplica para ellas también. Este documento sustituye a todas las políticas y regulaciones previas sobre uso aceptable para las Escuelas Públicas del Condado de Prince William.

I. Filosofía educacional de las PWCS

Las Escuelas Públicas del Condado de Prince William se comprometen a proporcionar una educación de primera clase para cumplir con las necesidades educacionales de nuestra diversa población estudiantil. El programa de instrucción en las PWCS se implementa por medio de un enfoque sistemático planificado que detalla el conocimiento y las habilidades a enseñar en cada material y en cada nivel de grado.

La tecnología es una herramienta valiosa que apoya y mejora el programa de instrucción de las PWCS al promover la solución de problemas, el pensamiento crítico, analítico y las habilidades de toma de decisiones. Los estudiantes y el personal tendrán acceso, procesarán y comunicarán la información en un ambiente dinámico, integrado y tecnológico.

II. Expectativa de privacidad

Los empleados y estudiantes no tienen expectativa de privacidad en el uso de las computadoras de la escuela o los servicios de Internet, ni el uso de las computadoras o medios relacionados de las PWCS crea un foro abierto o limitado conforme a la Primera enmienda a las constituciones federal o estatal. Cualquier expectativa de privacidad relacionada con el uso de aparatos que son propiedad del personal o del estudiante es denegada por la falta de cumplimiento con esta regulación u otras políticas y regulaciones de la Junta Escolar. La División retiene el derecho a monitorear toda la actividad de computadoras e Internet por parte de empleados y estudiantes y cualquier información o comunicación en los sistemas de computación y los servicios de red de las PWCS puede ser interceptado, grabado, leído, copiado y divulgado hacia el personal autorizado para propósitos oficiales, incluso investigaciones criminales. El uso de computadoras, redes y sistemas de Internet de las PWCS es un privilegio, no un derecho y puede ser retirado por la División en cualquier momento.

III. Usos aceptables de sistemas de computación y servicios de Internet de las PWCS

Es política general que los sistemas de computación y los servicios de Internet de las Escuelas Públicas del Condado de Prince William se proporcionen para propósitos administrativos, educacionales, de comunicación e investigación, congruentes con la misión, programa de estudios y objetivos de instrucción de la División. Las reglas y expectativas generales para el comportamiento y la comunicación profesional aplican al uso de las computadoras, redes y servicios de Internet de la División, así como aquellas reglas de conducta estudiantil establecidas en el Código de comportamiento de las PWCS. Los usos aceptables de los sistemas de computación y los servicios de Internet incluyen las actividades que apoyen la enseñanza y el aprendizaje. Las actividades aceptables como apoyo a este propósito incluyen, pero no se limitan al desarrollo profesional, las comunicaciones administrativas, las aplicaciones a becas, los anuncios de nuevos proyectos y las publicaciones de productos estudiantiles.

A. Uso aceptable por los empleados

Los empleados utilizarán las computadoras, las redes y los servicios de Internet de la División para propósitos relacionados con la escuela y el cumplimiento de sus tareas laborales. El uso personal incidental de computadoras escolares es permitido siempre que tal uso no interfiera con las tareas y el rendimiento del trabajo del empleado, con las operaciones del sistema u otros usuarios del sistema. El “uso personal incidental” se define como el uso por un empleado individual para comunicaciones personales ocasionales que no ocurran durante el horario de instrucción, cuyo uso no esté prohibido de alguna otra forma por esta regulación.

B. Usos inaceptables de los sistemas de computación y servicios de red de las PWCS

Cualquier infracción a la regulación no será tolerada y las PWCS actuarán rápidamente para corregir el asunto si la Regulación de uso aceptable y seguridad de Internet no se está siguiendo. Cualquier usuario que se detecte que ha violado esta regulación, la Regulación 295-2, Desarrollo del sitio web e Implementación, cualquier otra política o regulación que aplique de la Junta Escolar, o las provisiones aplicables del Código de Comportamiento de las PWCS, está sujeto a medidas disciplinarias, hasta e incluyendo la revocación de privilegio; disciplina estudiantil, hasta e incluyendo la expulsión; acción administrativa; disciplina de empleado, hasta e incluyendo el despido; y proceso criminal conforme a la ley local, estatal o federal que aplique.

C. Ejemplos de usos inaceptables de los sistemas de computación y servicios de red de las PWCS

La siguiente es una lista no exclusiva de ejemplos de acciones o actividades no aceptables:

1. Cualquier uso que sea ilegal o viole otras políticas o regulaciones de la Junta Escolar;

2. Violación de los derechos a la privacidad de cualquier estudiante o empleado;

3. Transmitir, descargar, almacenar o imprimir archivos o mensajes (texto, sonido, gráficas fijas o móviles, o cualquier combinación de los mismos) que sean pornografía o sean obscenos, conforme lo define el Código de Virginia §18.2-372, o que use lenguaje, sonidos o imágenes que sean lascivos o patentemente ofensivos (incluso “materiales visuales explícitamente sexuales” conforme lo define el Código de Virginia §18.2-374.1), o que degrade a otros (la administración invoca sus derechos discrecionales a determinar lo adecuado en circunstancias particulares);

4. Transmitir, descargar, almacenar, ver o imprimir archivos o mensajes (texto, sonido, gráficas fijas o móviles, o cualquier combinación de los mismos) que sean claramente ofensivos, lascivos, vulgares o que no sean congruentes con el plan de estudios y la misión educacional de las PWCS;

5. Acoso por computadora, lo que incluye transmisión de cualquier material o publicación de material en cualquier sitio web que sea amenazador para otra persona, o que tenga la intención de coartar, intimidar o acosar; material cuya intención sea comunicar lenguaje obsceno, vulgar, profano, lujurioso, lascivo o indecente, o que haga alguna sugerencia o propuesta de naturaleza obscena; o material que amenace con cualquier acto ilegal o inmoral, ya sea o no que tal material sea transmitido a esa persona ajena;

6. La División Escolar no tiene responsabilidad legal de regular o revisar los mensajes, las declaraciones, las publicaciones o los actos en Internet que sean fuera del campus, ni tampoco aquellos hechos en el campus utilizando un aparato propiedad del personal o del estudiante, que violen las regulaciones relacionadas con el uso de estos aparatos. Las PWCS se reservan el derecho a disciplinar a estudiantes y empleados por las acciones que realicen fuera del campus o utilizando equipo privado, las que pudieran violar esta Regulación si ocurren en las instalaciones o por medio del equipo de las PWCS, si tales acciones afectan adversamente la seguridad, el bienestar o el rendimiento de los estudiantes mientras están en la escuela, o en los buses escolares, en actividades escolares, o viniendo desde y hacia la escuela; si tales acciones amenazan con violencia contra otro estudiante o empleado; si tales acciones violan la ley local, estatal o federal, o las políticas o regulaciones de la Junta Escolar o el Código de Comportamiento, o si tales acciones interrumpen el ambiente de aprendizaje, administración o la conducta ordenada de la escuela. La División también puede tomar medidas disciplinarias adecuadas, hasta e incluyendo el despido, por actividades en Internet fuera del campus, que sean incongruentes con las normas profesionales y éticas esperadas de los empleados de las PWCS como "modelos ejemplo" para los estudiantes de las PWCS.

7. Copiar o instalar información confidencial, incluso software, violando los acuerdos de licencias de software y la ley correspondiente;

8. Se prohíbe estrictamente copiar sin autorización material con derechos reservados incluso, pero sin limitarse únicamente a la digitalización y distribución de fotografías de revistas, libros u otras fuentes con derechos reservados, música o videos con derechos reservados y la instalación de cualquier software con derechos reservados para los que las PWCS y el usuario final no tienen una licencia activa;

9. Utilizar la red de las PWCS o la información contenida en la red para ganancia financiera personal, comercial, propaganda, requerimientos o actividad comercial que no sea en nombre de las Escuelas Públicas del Condado de Prince William, a menos que sea autorizado bajo la Regulación 923-1, Propaganda comercial, o cualquier actividad ilegal;

10. Cualquier uso para un foro para comunicarse por correo electrónico o cualquier otro medio con otros usuarios de la escuela o personas ajenas para hacer requerimientos, proselitismo, defensa o comunicar los puntos de vista de una persona o una organización no patrocinada por la escuela; para solicitar membresía o apoyo en alguna organización no patrocinada por la escuela; o para recolectar fondos para cualquier propósito no patrocinado por la escuela, ya sea que haya ganancia o no haya ganancia. Ningún empleado proporcionará a sabiendas nombres, direcciones de correo electrónico u otra información personal a personas externas cuya intención sea comunicarse con los empleados de la escuela, los estudiantes o sus familias para propósitos que no sean de la escuela. Los empleados que no estén seguros sobre si ciertas actividades particulares son aceptables, deberán buscar dirección de su supervisor o del Director de Tecnología de la Información;

11. Enviar correos electrónicos masivos a usuarios de la escuela o personas ajenas para propósitos de la escuela o ajenos, sin el permiso de un administrador;

12. Uso de la red de las PWCS para propósitos políticos, incluso cualquier uso que requiera que los estudiantes lleven o entreguen cualquier material que (a) defienda la elección o rechace a cualquier candidato para un puesto oficial; (b) defienda la aprobación o rechazo de cualquier pregunta para el referendo; o (c) defienda la aprobación o rechazo de cualquier asunto pendiente ante la Junta Escolar, la Junta de Supervisores del Condado, o la Asamblea General de Virginia, o el Congreso de los Estados Unidos;

13. Cualquier intento de tener acceso no autorizado a los sitios;

14. Cualquier intento para eliminar, borrar o de cualquier otra forma esconder cualquier información almacenada en una computadora de la escuela, que viola estas reglas, o en cualquier momento después de haber sido notificado por un administrador o supervisor que conservara cualquier material almacenado en una computadora de la escuela;

15. Tratar de degradar o interrumpir el sistema, deliberadamente, o el rendimiento de la red. Tales actos también serán vistos como actividad criminal bajo las leyes estatales y federales que apliquen;

16. Transmitir o mostrar mensajes que promuevan la venta de productos y servicios, excepto como se indica en la Regulación 923-1, Propaganda comercial.

17. Intentos de modificar instalaciones del sistema, descargar o transmitir virus de anexos a correo electrónico o cualquier otra fuente, obtener ilegalmente recursos adicionales, o tratar de trastocar las restricciones asociadas con cualquier sistema de computación, cuenta de computación, servicio de red o software de protección de computadoras personales;

18. Escribir contraseñas y almacenarlas en cualquier lugar que sea accesible para otros. Guardar contraseñas en un archivo de CUALQUIER sistema de computación (incluso las PDA o dispositivos similares) sin encriptado;

19. Volver a publicar comunicaciones personales sin el consentimiento previo del autor;

20. Transmitir mensajes no solicitados por correo electrónico o cartas de cadenas que de otra forma serían incongruentes con el plan de estudios y la misión educacional de las PWCS;

21. Uso personal no relacionado con propósitos educacionales o administrativos;

22. Recolecta de dinero o vínculos hacia información de recolectas de dinero en sitios web de la escuela o del departamento o la página web de las Escuelas Públicas del Condado de Prince William, a menos que explícitamente esté autorizado como parte de las actividades de las PWCS.

23. Enviar información confidencial y clasificada de las PWCS a personas no autorizadas, o publicar esta información fuera de las PWCS;

24. Distribución de cualquier mapa del interior de la escuela, planes de piso, o descripciones escritas de los planes interiores de pisos en páginas web, ubicaciones de las cámaras, o cualquier otra información que podría comprometer la seguridad de la escuela;

25. Conectar un equipo de computación que no sea de las PWCS a la red de las PWCS o equipo de computación por otro medio que no sea la Red Inalámbrica para invitados.

26. Cualquier contenido prohibido por la Regulación 295-2, Desarrollo del sitio web e Implementación.

IV. Uso aceptable de dispositivos de comunicación inalámbrica de propiedad personal

Como reconocimiento de la creciente importancia y utilidad de los dispositivos de comunicación inalámbrica (teléfonos inteligentes, tabletas, lectores electrónicos, etc.) el uso de estos dispositivos de propiedad personal, de parte de estudiantes y empleados, será permitido dentro de las escuelas y clases de las PWCS, siempre que su uso cumpla con las reglas establecidas a continuación, en el Código de Comportamiento y por los Directores y maestros en la implementación basada en la escuela de esta Regulación.

Los Directores establecerán y comunicarán reglas específicas que regularán el uso de dispositivos de comunicación inalámbrica de propiedad personal en cada escuela, para incluir pero no limitarse a los horarios y ubicaciones de uso aceptable. Como se considere adecuado, los Directores pueden delegar a los maestros de clases la autoridad de establecer reglas especiales o prohibiciones de uso durante situaciones específicas de clase.

Todas las reglas de la escuela y la clase incorporarán los siguientes reglamentos:

1. La posesión de dispositivos de comunicación por los estudiantes o el persona en los terrenos de las PWCS es un privilegio, no un derecho, y cualquier miembro del personal o estudiante que traiga un dispositivo de comunicación a la propiedad de las PWCS acepta estas reglas y el derecho de la División Escolar de confiscar o revisar tales dispositivos, conforme lo indican estas reglas;

2. Todos los dispositivos deben colocarse en modo silencioso o de vibración, con todas las señales audibles deshabilitadas durante todo el uso dentro de la escuela;

3. Las configuraciones de bocinas deben estar apagadas. El contenido en audio debe ser presentado por medio de audífonos para prevenir cualquier interrupción de las actividades escolares;

4. Las protecciones específicas se requieren para asegurar la integridad de las pruebas académicas. En cada situación específica de pruebas, los Directores o maestros de clases establecerán y declararán en forma afirmativa las reglas específicas que regulan el uso de dispositivos en esas circunstancias. Por ejemplo, el uso de una aplicación de calculadora puede ser permitida en ciertas pruebas de matemática o ciencias, mientras que todas las aplicaciones de comunicación deben deshabilitarse; un maestro puede determinar que todos los dispositivos deben apagarse; o los Directores u Oficiales de división pueden prohibir el uso de dispositivos en todas las áreas de la escuela durante exámenes principales estandarizados o periódicos.

5. La violación de cualquier restricción específica de uso de dispositivos que se observe durante la prueba puede considerarse como engaño y será castigado como tal. Cualquier uso de dispositivos de comunicación electrónica para la transmisión o recepción de preguntas de las pruebas, respuestas u otro contenido protegido, también será considerado engaño;

6. Los dispositivos de comunicación inalámbrica pueden utilizarse en los buses escolares siempre que el dispositivo no distraiga al conductor, comprometa la seguridad o viole otras reglas o regulaciones del bus escolar. Los violadores de estas regulaciones serán sujetos a la confiscación del dispositivo de comunicación u otra acción correctiva;

7. Pueden llevarse a cabo búsquedas de dispositivos de comunicación si el administrador tiene una sospecha razonable de que se está utilizando para una conducta que es criminal o una violación del "Código de Comportamiento" o el "Código de Conducta del Empleado", conforme aplique.

8. PWCS no asume responsabilidad por la seguridad de la comunicación o dispositivos electrónicos que se hagan en la propiedad de las PWCS;

9. Mientras se encuentran en la propiedad de la escuela, en cualquier actividad relacionada con la escuela, o mientras viaje de y hacia la escuela o a cualquier otra actividad relacionada con la escuela, los estudiantes no tomarán o mostrarán gráficos de video o imágenes fijas de una persona que no esté vestida o que esté parcialmente vestida. Las personas estarán sujetas a acción disciplinaria, hasta e incluyendo la expulsión. Conforme al Código de Virginia, § 18.2- 386.1, este crimen es un delito menor si la víctima es un adulto, pero es un delito grave si la víctima es menor a 18 años;

10. Mientras se está en propiedad de la escuela, en cualquier actividad relacionada con la escuela, o mientras viaje de y hacia la escuela o a actividades relacionadas con la escuela el uso de dispositivos inalámbricos está sujeto a todos los términos del "Código de Comportamiento" y el "Código de Conducta del Empleado"; y

11. La División Escolar no puede monitorear ni responsabilizarse por las comunicaciones o acciones originadas en dispositivos de propiedad personal utilizados en propiedad de las PWCS.

V. Áreas de responsabilidad

Los empleados, estudiantes, contratistas, consultores, empleados temporales de las PWCS, incluso todo el personal afiliado con terceros, voluntarios en las PWCS y todas las otras personas a las que se les otorga acceso a la infraestructura de la red de las PWCS deben cumplir con, y son responsables por monitorear, hacer cumplir y reportar las infracciones a la Política de uso aceptable de las PWCS.

- Los Gerentes de la Oficina Central (es decir, el supervisor del departamento o el director) y los Directores y los otros administradores con base en la escuela serán responsables de asegurar que se sigan estas Política de uso aceptable y Regulaciones 923-1, Propaganda comercial, y la 295-2, Desarrollo del sitio web e Implementación.

  Los administradores también monitorearán el uso por los maestros y supervisarán la integración correcta de la tecnología en la instrucción.

- Los Gerentes web dentro de las escuelas y los departamentos de la oficina central también serán responsables de asegurar que se sigan estas Política de uso aceptable y Regulaciones 923-1, Propaganda comercial, y la 295-2, Desarrollo del sitio web e Implementación.

- Los maestros serán responsables de guiar y monitorear el uso de los estudiantes de los sistemas de computación de las PWCS y los servicios de red y proporcionar instrucciones de seguridad de Internet a los estudiantes.

- Los estudiantes serán responsables por el cumplimiento de la Política de uso aceptable y seguridad de Internet de las PWCS y la regulación y el uso de sistemas de computación de las PWCS y los servicios de red para las tareas directamente relacionadas con el programa de estudios.

- Los padres serán responsables de asegurar que sus hijos cumplen la Política de uso aceptable de las PWCS y la regulación y el uso de sistemas de computación de las PWCS y los servicios de red para las tareas directamente relacionadas con el programa de estudios.

VI. Seguridad

A. Medidas de protección de la tecnología.

Hasta donde sea práctico, las medidas de protección de la tecnología (o "filtros de Internet") se utilizarán para bloquear o filtrar el Internet u otras formas de acceso a información inadecuada por comunicaciones electrónicas. Específicamente, conforme lo requiere la Ley de protección de Internet para los niños [Pub. L. No. 106554 y 47 USC 254(h)], el bloqueo se aplicará a las muestras visuales de material considerado obsceno o pornografía infantil, o a cualquier material que se considere dañino para los menores de edad. Sujeto a supervisión del personal y a la aprobación del Director de Servicios de Tecnología de la Información o su representante, pueden deshabilitarse las medidas de protección de tecnología o, en caso de menores de edad, minimizarse para una investigación de buena fe o para otros propósitos legales. Los Servicios de Tecnología de la Información de las Escuelas Públicas del Condado de Prince William han implementado y mantienen las tecnologías líderes de la industria para asegurar y proporcionar acceso seguro de Internet para los estudiantes y el personal. Los complementos de filtros de Internet de la estrategia general de seguridad de las Escuelas Públicas del Condado de Prince William con el uso de un enfoque holístico para proteger la propiedad de los estudiantes, empleados y redes. Las PWCS filtran y monitorean la actividad de Internet por medio de medidas protectoras de tecnología utilizadas para bloquear o filtrar el Internet u otras formas de comunicaciones electrónicas. Los filtros se aplicarán a todos los materiales que se consideren inadecuados, conforme a las leyes aplicables. Sujeto a la supervisión del personal, se pueden evitar las medidas de protección o, en el caso de los menores, medidas minimizadas, para una investigación de buena fe u otros propósitos legales. Se debe obtener autoridad para obviar o modificar cualquier medida de protección de tecnología del Director de Servicios de Tecnología de la Información o su representante designado. Será responsabilidad de todo el personal de las Escuelas Públicas del Condado de Prince William supervisar y monitorear el uso de la red de computadoras y el acceso a la Internet conforme a las leyes federales y estatales aplicables, los lineamientos y las regulaciones del Departamento de Educación de Virginia y las políticas y regulaciones de la Junta Escolar.

B. Privacidad de datos de empleados y estudiantes

Estas normas se estructuran para proporcionar la diligencia y cumplimientos acordes a las leyes federales, estatales y locales que aplican, así como las políticas y regulaciones de la Junta Escolar, para la protección de la información confidencial y la privacidad de la información de los estudiantes y empleados durante la recopilación, transferencia, almacenamiento, uso, divulgación y destrucción de tal información. Para proteger la privacidad de los empleados y los estudiantes, el personal del sistema escolar es legalmente responsable por salvaguardar la información recopilada relacionada o proveniente de los empleados y estudiantes. Los datos deben almacenarse intactos evitando accidentes, acceso no autorizado, robo, cambios no autorizados o divulgación no intencional. Las personas que manejan los datos deben comprender lo que se considera acceso adecuado e inadecuado a los datos y su uso consiguiente. Los cambios, alteraciones y la distribución de los datos se pueden hacer solo en las formas autorizadas y aceptables. No puede utilizarse una solución encriptada o un programa de compartir archivos a menos que sea autorizado o aprobado por el Director de Servicios de Tecnología de Información o su representante.

La recopilación, uso y divulgación de información del estudiante o del empleado que pueda identificarles personalmente estará estrictamente limitada a propósitos educacionales y administrativos de buena fe. Las fotos y nombres de estudiantes y personal se permiten en los sitios web de las PWCS con el propósito de hacer publicidad a las actividades escolares o a los logros estudiantiles, pero tal información debe utilizarse con precaución y conforme a la Regulación 790-4, Divulgación de información del directorio, lo que da a los estudiantes y a sus padres y tutores el derecho de denegar la divulgación pública de sus nombres, fotos y otra información del estudiante. La información relacionada con los estudiantes individuales solo puede utilizarse si cumple con la definición de información del directorio contenida en la Regulación 790-4 y si el estudiante, padre de familia o tutor no ha optado por denegar tal divulgación.

Los números de seguridad social no pueden ser recopilados ni divulgados a menos que lo autorice la ley. La información personal, tal como nombres, títulos y descripciones de puestos, números de teléfono y facsímil, dirección de correo electrónico y otras, pueden ser recopiladas y utilizadas internamente para la inscripción en el programa o seminario de las PWCS por medio de Internet u para la participación de programas en línea de las PWCS u otros propósitos legítimos de las PWCS. Tal información no se venderá o compartirá con ningún grupo externo ni se divulgará a cualquier tercero ajeno a las PWCS.

Los archivos conteniendo datos confidenciales o sensibles no pueden ser almacenados en medios portátiles o dispositivos móviles que salgan de la propiedad de las PWCS, a menos que lo apruebe el gerente de departamento de la oficina central, el director de la escuela, y protegidos por una solución encriptada aprobada por los Servicios de Tecnología de la Información.

Las personas o compañías bajo contrato con las PWCS pueden tener acceso a la información en el curso del servicio que proporcionan a las PWCS, pero estas entidades no tienen permitido el uso o divulgación de esa información para propósitos no autorizados y deben firmar un acuerdo de no divulgación de las PWCS antes de que el trabajo se lleve a cabo. Ninguna otra entidad está autorizada a recopilar información por medio de los sitios se las PWCS.

Todos los sistemas basados en la web, hospedados en los sistemas de las PWCS o de un proveedor, que interactúen con la información de estudiantes, empleados o las PWCS, deben proporcionar un protocolo seguro para el acceso y autenticación al sistema y haber llenado el formulario de normas de seguridad del proveedor de servicios así como el acuerdo de no divulgación. Tales sistemas proporcionarán un FTP seguro o un protocolo equivalente para cualquier transferencia necesaria de datos o para interfaces entre los sistemas, si aplicara.

Se debe notificar inmediatamente el Manejo de riesgos si hay información sensible o crítica de las PWCS que se comprometa o se pierda, si se divulga a personas no autorizadas, o si se sospecha que se ha perdido o divulgado a personas no autorizadas, o si cualquier uso no autorizado de los sistemas de información de las PWCS se ha dado o se sospecha que se haya dado.

C. Acceso a los sistemas de computación de las PWCS y los servicios de red

Los empleados, estudiantes y empleados temporales de las PWCS aceptan su comprensión de la Política de uso aceptable y seguridad de Internet como condición para recibir acceso al sistema de computación y servicios de redes. Se recordarán a todos los empleados las expectativas de Uso aceptable de las PWCS, anualmente, en los boletines de empleados (es decir, "Communicator" Comunicador y "the Leader" el Líder). Los administradores del edificio y los supervisores del departamento serán responsables de revisar las expectativas con su personal.

D. Cuentas de usuarios

Todos los servicios de aplicaciones, correo electrónico, a nivel de sistema y a nivel de usuario deben tener una identificación única de usuario. Los usuarios no permitirán que otros tengan acceso a su cuenta y son responsables de todas las actividades llevadas a cabo con su cuenta. Además, los empleados y estudiantes no deben usar las cuentas de otros para llevar a cabo actividades con los recursos de información de las PWCS. Es responsabilidad del usuario asegurarse que su identificación no se comparte con otros. Se llevará a cabo una revisión trimestral de las cuentas de usuarios para eliminar las cuentas vencidas de usuarios y para asegurar el cumplimiento de esta regulación.

- No deben utilizarse cuentas de correo electrónico, aplicaciones o redes genéricas y temporales, a menos que lo apruebe el Director de Servicios de Tecnología de la Información o sus representantes designados.

- No se permitirá a los usuarios más de una sesión concurrente y el acceso estará restringido al horario laboral de las PWCS, a menos que lo autorice el Director de Servicios de Tecnología de la Información o sus representantes.

- Se requiere que los empleados cierren sus sesiones de computación todos los días y antes de permitir que otro usuario tenga acceso a un sistema de computación en el que ellos tengan una sesión activa. Los empleados serán responsables de cualquier uso no autorizado de una computadora, red o sistema de Internet, que haga cualquier persona o estudiante que tenga acceso debido a que el empleado no haya cerrado su sesión como se requiere.

- Los usuarios de computadoras portátiles primero deben ingresar a la red de las PWCS por medio de su cuenta de ingreso a la red para crear una cuenta de usuario local en el sistema de la computadora portátil para proporcionar acceso y responsabilidad sobre el uso mientras no están en las instalaciones.

E. Autenticación

La autenticación es un método utilizado para validar una autorización de usuario para tener acceso a un sistema o aplicación de computación. Los usuarios se adherirán a los siguientes procedimientos de autenticación:

- Los sistemas de computación del empleado y del administrador utilizarán un descansador de pantalla aprobado por las PWCS, con la característica de "contraseña para reanudar el trabajo" requerida después de 10 minutos.

- Los usuarios asegurarán los sistemas de computación por medio de descansadores de pantalla protegidos con contraseñas cuando se retiren de los sistemas de computación. Esta característica previene el uso no autorizado de un sistema de computación después de que un usuario legítimo se registre, pero se retire momentáneamente de su computadora. Se excluyen las computadoras del público y de los estudiantes, como las que se encuentran en la biblioteca o en los laboratorios, ya que no tienen información crítica o sensible.

- Se requieren cierres de sesiones de no más de cinco minutos para las aplicaciones basadas en la web.

- Los sistemas de computación conectados a una red y los servicios de aplicación en la web, propiedad de las PWCS, tendrán un letrero de advertencia en todos los puntos de acceso y se asegurarán que se muestre el letrero cada vez que el sistema se enciende o un usuario ingresa.

F. Contraseñas

Una contraseña se utiliza en conjunto con una identificación única de usuario para autenticar el derecho de un usuario a tener acceso a un sistema de computación y un servicio de aplicación. Las contraseñas ayudan a proteger contra el uso inadecuado ya que buscan restringir el uso de los sistemas y redes de las PWCS a usuarios no autorizados. Los usuarios autorizados son responsables de la seguridad de sus contraseñas y cuentas. Las contraseñas se consideran secretas y no deben compartirse bajo ninguna circunstancia. Las contraseñas de usuarios individuales nunca deben estar integradas a una aplicación o proceso. Todas las contraseñas de servicios de aplicación, correo electrónico, a nivel de sistema y a nivel de usuario, deben cumplir con estos lineamientos. Las computadoras públicas, como las que están en la biblioteca o en los laboratorios, sin información crítica o sensible, pueden estar excluidas caso por caso, si lo aprueba el Director de Servicios de Tecnología de la Información o sus representantes designados.

Debe asignarse una contraseña a cada identificación única de usuario. Se requiere que los usuarios cambien su contraseña inmediatamente después de que se registren por primera vez en el sistema o en la aplicación.

Si una cuenta o contraseña es sabida o se sospecha que se ha perdido, se la han robado o se ha divulgado, el usuario debe reportar inmediatamente el incidente al Director de Servicios de Tecnología de la Información o a sus representantes designados y cambiar todas las contraseñas. Los requerimientos para las contraseñas se encuentran en el Anexo III.

G. Recursos de comunicación electrónica

Se asignan a los empleados cuentas de correo electrónico de las PWCS, a ser utilizadas para propósitos educacionales y para la comunicación oficial de la División de las PWCS. Debe deshabilitarse el direccionamiento automático de mensajes de correo electrónico, a menos que lo autorice el Director de Servicios de Tecnología de la Información o sus representantes designados para prevenir que la información confidencial y clasificada se divulguen a personas o entidades no autorizadas.

Si se asignan a los estudiantes cuentas de correo electrónico, blog, foro de discusión, cuentas de medios sociales o cualquier otra forma de comunicación electrónica, el patrocinador debe ser un maestro. Los patrocinadores son responsables de guiar y monitorear la comunicación de los estudiantes y el uso de las secciones de la red que sean adecuadas y de asegurarse que los estudiantes comprendan que el uso inadecuado de la red causará que pierdan sus cuentas o que enfrenten acciones disciplinarias. Cuando sea adecuado, los patrocinadores asumirán la responsabilidad de enseñar a los estudiantes las técnicas y normas adecuadas para su participación; explicar los temas de privacidad, infracción de derechos de autor, uso de la herramienta y etiqueta en la red.

H. Equipos y software

El software utilizado por las escuelas o los departamentos individuales diseñados para ser usados en la red de las PWCS debe ser revisado por el Comité de dirección de tecnología de la información antes de ser comprado o instalado y debe ser aprobado por el Director de Servicios de Tecnología de la Información o su representante. El Departamento de Servicios de Tecnología de la Información es responsable de obtener y verificar la autorización escrita adecuada de los dueños del sistema de información para dar acceso al sistema o a los recursos de las aplicaciones que se hayan implementado en la red conectada a los sistemas de computación. Los usuarios finales no pueden instalar, llevar a cabo o descargar software o modificar las configuraciones de la red conectada a los sistemas de computación, a menos que tengan autorización de Servicios de Tecnología de la Información. Esta estipulación existe para asegurar el cumplimiento de las leyes de derechos reservados, la administración de parches, evitar el software malicioso y para la infraestructura en general y la integridad del sistema de computación. La instalación de computadoras conectadas a la red, su reparación, actualización incluso de equipo y el software deberá ser aprobada, dirigida y completada por Servicios de Tecnología de la Información.

El software que protege de virus o software malicioso, de la División, debe ser instalado, activado y mantenido actualizado en todos los sistemas de computación conectados a la red en todo momento. El software que protege de virus o software maligno debe ser administrado centralmente y no debe ser configurable por los usuarios finales. Deben llevarse a cabo escaneos semanales del sistema en todos los sistemas de computación. Los sistemas de computación infectados con software malicioso deben ser remediados inmediatamente o eliminados de la red hasta que sea verificado como libre de software malicioso.

Conforme se descubran nuevas vulnerabilidades y conforme haya disponibilidad de actualizaciones en software, los sistemas de computación deberán tener los parches de seguridad de software que sean adecuados y que hayan surgido recientemente, proporcionales al nivel identificado de riesgo aceptable.

Todos los sistemas (es decir, computadoras, monitores e impresoras) deberán ser apagados al final del día escolar o laboral y en los días en que la escuela y las oficinas estén cerradas, a excepción de los días u horas establecidos para permitir los escaneos del sistema que protege de virus o software malicioso que se hacen en horario extraordinario, así como mantenimiento o actualización de parches de sistemas operativos o software (es decir, dejar las computadoras encendidas todas las noches de miércoles y jueves). En algunas ocasiones, se puede indicar a las escuelas u oficinas que dejen sus computadoras encendidas por razones especiales o asuntos urgentes relacionados con actualizaciones o asuntos de seguridad de datos, que deben ser tratados inmediatamente.

I. Acceso remoto

Es responsabilidad de los empleados, contratistas, proveedores y agentes de las PWCS que tengan privilegios de acceso remoto a la red de las PWCS, asegurarse que su conexión de acceso remoto tenga la misma consideración que la conexión del usuario en las instalaciones de las PWCS. Todos los usuarios que necesiten acceso remoto para equipos de las PWCS deberán utilizar herramientas administradas centralmente y cumplir con las Normas de firewall de Servicios de Tecnología de la Información. Las organizaciones o personas que deseen implementar soluciones no estándar de acceso remoto a la red de PWCS deberán obtener autorización del Director de Servicios de Tecnología de la Información o su designado. Todos los sistemas de computación que estén conectados a la red interna de las PWCS por medio de tecnología de acceso remoto deben cumplir con todos los requerimientos de esta regulación.

VII. Respuesta, mitigación, administración e investigación de incidentes

La respuesta a incidentes busca facilitar el descubrimiento, administración, mitigación, investigación y consciencia de incidentes de seguridad relacionados con el sistema de computación y el servicio de red, de forma que cumpla con las leyes, políticas y regulaciones aplicables. Todos los incidentes identificados relacionados con la seguridad deben ser reportados inmediatamente al administrador del sitio o al Departamento de Manejo de Riesgos de las PWCS. El Departamento de Manejo de Riesgos de las PWCS o el Director de Servicios de Tecnología de la Información o sus representantes designados verificarán que haya ocurrido un incidente y determinarán qué acción necesita tomarse, si es necesario (Anexo III). Ningún usuario encenderá o apagará, desconectará, eliminará información o interrumpirá en otra forma cualquier computadora sujeta a decomiso, a menos que sea bajo la dirección de Manejo de Riesgos o del Director de Servicios de Tecnología de la Información, o sus representantes designados.

VIII. Conservación de evidencia electrónica

Cuando la División tiene un aviso de una litigación real o anticipada, es necesario conservar toda la evidencia, incluso la evidencia electrónica, relacionada con tal litigación. Los empleados que reciben aviso de las PWCS de una licitación real o que se amenaza (o escuchan de otras fuentes acerca de tal litigación real o que se amenaza) deben conservar toda esa evidencia y no pueden eliminar, alterar o interrumpir de ninguna manera la integridad de cualquier evidencia electrónica. Esto incluye, pero no se limita a correo electrónico, archivos, carpetas y cualquier otro dato o comunicación electrónica.

IX. Instrucción de seguridad de Internet

La instrucción de seguridad de Internet es responsabilidad de todo el personal de instrucción. “NetSmartz”, el programa de estudios sobre seguridad en Internet, que va desde kindergarten hasta décimo segundo grado, proporcionado por el Centro nacional para niños desaparecidos y explotados y se utilizarán recursos adicionales con estudiantes de todos los niveles de grado.

El plan de instrucción de Seguridad en Internet puede encontrarse en el Anexo III.

X. Proceso de revisión

El Superintendente Asociado de los Servicios de Comunicaciones y Tecnología (o su representante) es responsable de implementar y supervisar esta regulación y la Política de uso aceptable.

El Superintendente Asociado de los Servicios de Comunicaciones y Tecnología (o su representante) es responsable de revisar esta regulación y la Política de uso aceptable, en forma anual, con la ayuda del Departamento de Servicios de Tecnología de la Información de las PWCS y la Oficina de Tecnología de Instrucción. Cada dos años, el Superintendente de la División presentará una Política de uso aceptable ante el estado, que haya sido aprobada por la Junta Escolar de las PWCS.

ANEXO I:

Recursos

Contactos para incidentes de seguridad

- Administrador del sitio, Director, consejero o supervisor del departamento
- Manejo de Riesgos y Servicios de Seguridad 703.791.7206
- Departamento de Servicios de Tecnología de la Información 703.791.8722

Código de Comportamiento de las Escuelas Públicas del Condado de Prince William en el sitio web de las PWCS (pwcs.edu)

ANEXO II

Requisitos de contraseñas

- Caracteres mínimos: 8
- Las contraseñas deben contener al menos una letra, un numeral y un carácter especial
- No pueden repetirse caracteres ni escribirse en forma consecutiva
- Contener caracteres en mayúsculas y minúsculas (es decir, a-z, A-Z)
- Contener caracteres numéricos y especiales, tales como 0-9, !@#$%^`&*()
- La contraseña no debe contener una palabra que se encuentre en el diccionario (de inglés)
- Configuraciones de expiración: al menos una vez cada seis meses
- Ninguna de las 3 contraseñas previas del usuario pueden ser usadas nuevamente
- Las cuentas deben bloquearse automáticamente después de tres intentos consecutivos fallidos de ingreso, durante al menos 30 minutos, para detener suficientemente la piratería de contraseñas con fuerza bruta con contraseñas fuertes habilitadas

ANEXO III:

Plan de instrucción de seguridad de Internet

Programa de implementación

Abril de 2007	Investigación y desarrollo del programa de Seguridad de Internet y el plan de implementación. Revisar el programa de estudios "NetSmartz".
Mayo de 2007	
Septiembre a diciembre de 2007	Determinar conceptos que serán enseñados en los niveles específicos de los grados y desarrollar cualquier recurso adicional que se necesite. Desarrollar un curso en línea que pueda ser accesado por los maestros y administradores.
Diciembre de 2007	Desarrollo profesional para maestros de recursos de tecnología de instrucción. Seleccionar escuelas para hacer el plan piloto del programa de estudios.
Enero a febrero de 2008	Proporcionar desarrollo personal y en línea para maestros que harán el plan piloto del programa de estudios.
Febrero a abril de 2008	Hacer el plan piloto del programa de estudios en escuelas seleccionadas.
Mayo a junio de 2008	Evaluar el programa del plan piloto.
Agosto de 2008	Reportar los resultados del plan piloto al DOE de Virginia
Septiembre de 2008	Presentar el reporte al DOE de Virginia con AUP y el programa revisado de Seguridad de Internet.
	Implementación completa del programa de Seguridad de Internet.

Desarrollo profesional

Verano de 2007	Entrenamiento sobre Regulación del uso aceptable para el personal administrativo.
Septiembre de 2007	Entrenamiento basado en el sitio sobre Regulación del uso aceptable para el personal de la escuela.
Anualmente en septiembre	Revisión anual de AUP por todo el personal de las PWCS.
Diciembre de 2007	Desarrollo profesional para maestros de recursos de tecnología de instrucción.
Enero a febrero de 2008	Desarrollo profesional personal y en línea para escuelas que serán el plan piloto para el programa de estudios de Seguridad de Internet.
Primavera de 2008	Desarrollo profesional personal y en línea para todas las escuelas.

Alcance a la comunidad y entrenamiento

- Presentación de Seguridad de Internet en la Exhibición anual de tecnología
- Reuniones de padres de familia y la comunidad, en la escuela
- Colaboración con el Departamento de Policía del PWC y los Oficiales de Recursos Escolares para desarrollar protocolos y programa de estudios de la seguridad de Internet
- Uso de las comunicaciones públicas disponibles (red de televisión de las PWCS) para proporcionar información sobre seguridad de Internet a padres de familia y a la comunidad