REGLAMENTO MONTGOMERY COUNTY PUBLIC SCHOOLS

Registros Relacionados: BBB, EDC, EDC-RA, EGI-RA, EHC-RA, IGS, JFA, JFA-RA, JHF-RA, JOA-RA, KBA-RB, KBB

Oficinas Responsables: Superintendente de Escuelas (Superintendent of Schools)

Responsabilidades del Usuario para Sistemas de Computación, Información Electrónica y Seguridad de la Red

I. PROPÓSITO

A. Garantizar la seguridad de todos los elementos del sistema de computación de Montgomery County Public Schools (MCPS) relacionados con la tecnología y la información electrónica;

B. Delinear los usos apropiados para todos los usuarios de sistemas de computación de MCPS;

C. Promover el desarrollo intelectual a través del uso de sistemas de computación, tecnología relacionada e información electrónica en un entorno seguro; y

D. Garantizar el cumplimiento de las leyes estatales, locales y federales relevantes.

II. ANTECEDENTES

MCPS proporciona equipos y servicios de computación y acceso a la red a las escuelas y oficinas para fines que concuerden con la misión de MCPS. La amplia gama de tecnología informática disponible para los usuarios de MCPS presenta nuevos riesgos y oportunidades. La responsabilidad por el comportamiento apropiado reside en todas las personas que utilizan los recursos de tecnología informática y acceso a computación de MCPS. En las escuelas, las actividades de los menores en línea son monitoreadas por el personal y a través de medidas de protección tecnológica en todo el sistema escolar. Los niveles de acceso se proporcionan según la tarea, la responsabilidad y la necesidad de saber o conocer. Los usuarios deben proteger la información y los recursos contra robo, daño malicioso, acceso no autorizado, manipulación y pérdida.

III. DEFINICIONES

A. Un *método aprobado de firma electrónica* es aquel que ha sido aprobado por el superintendente de escuelas y/o su designado, conforme a este reglamento y todas las leyes estatales y federales aplicables, y que especifica la forma de la firma electrónica, los sistemas y procedimientos usados con la firma electrónica y el significado del uso de la firma electrónica.

B. Un *sistema de computación* es hardware, software y tecnologías relacionadas, incluidos redes, cableado y equipos de comunicación.

C. *Ciberacoso y/o hostigamiento o intimidación electrónica* significa conducta intencional usando comunicación electrónica tal como correo electrónico, mensajes instantáneos, sitios sociales, blogs, teléfonos móviles u otros métodos tecnológicos para crear un entorno educativo hostil al interferir sustancialmente con los beneficios educativos, las oportunidades o el desempeño de un estudiante, o con el bienestar físico o psicológico de un estudiante, y:

- Está motivada por una característica personal real o percibida, incluyendo raza, origen nacional, estado civil, sexo, orientación sexual, identidad de género, religión, ancestro, atributos físicos, condición socioeconómica, condición familiar o capacidad o discapacidad física o mental

- Es amenazante o gravemente intimidatoria

- Se produce en una instalación escolar, durante una actividad o evento escolar o en un autobús escolar

- Interfiere sustancialmente con el funcionamiento ordenado de una escuela

D. *Fines educativos* son aquellas acciones que promueven directamente las misiones educativas, docentes, administrativas, comerciales y de servicios de apoyo de MCPS y relacionadas con cualquier tipo de enseñanza, proyecto, trabajo, asignación de trabajo, tarea o función que sea la responsabilidad del usuario.

E. *Datos e información electrónica* son datos o figuras en cualquier formato electrónico o digital. Ejemplos incluyen correo electrónico, mensajes instantáneos, salas de charla (chat), mensajes de texto, documentos, bases de datos, archivos, sitios web y cualquier otra información almacenada electrónicamente.

F. Un *registro electrónico* es información generada, enviada, recibida o almacenada en formato digital relacionada con la conducta comercial de MCPS, comunicada entre las partes como evidencia de una transacción y conservada para fines de

documentación de MCPS. Un registro no incluye información cuyo carácter es tan transitorio que ordinariamente no se conservaría.

G. Una *firma electrónica* es un sonido, símbolo o proceso anexado a, o lógicamente asociado con, un registro electrónico y ejecutado o adoptado por una persona con la intención de firmar un registro.

H. *Materiales inapropiados* son materiales que son obscenos o pornográficos y por lo tanto dañinos a los menores/estudiantes, incluyendo sitios web relacionados con contenido adulto/sexualmente lascivo, materiales que no son apropiados según la edad y materiales sin un fin educativo, según se define en este reglamento o que no concuerdan con la seguridad del sistema o las políticas y reglamentos de MCPS. Materiales inapropiados podrían también incluir aquellos que promueven o avanzan la piratería (hacking); el uso, distribución y producción de drogas, alcohol y tabaco; acoso, hostigamiento e intimidación; aptitudes criminales, violencia o uso ilegal o posesión de armas. Donde la necesidad de legítima investigación u otro fin lícito sea identificada por el personal, se podría otorgar acceso apropiado.

I. *Acceso a Internet* incluye todos los métodos autorizados que se usan para conectar a los servidores y usuarios de Internet y todos los métodos autorizados para proveer acceso.

J. Una *medida de protección tecnológica* es una tecnología de filtrado de material de Internet que está diseñada para limitar el acceso a sectores seleccionados de Internet basado en criterios identificados diseñados para limitar o prevenir el acceso a material inapropiado.

K. *Equipo no autorizado* es cualquier dispositivo que no esté aprobado por la Oficina del Jefe de Tecnología (Office of the Chief Technology Officer–OCTO) y/o su designado para estar conectado a una computadora de MCPS o a la red de MCPS, incluyendo, pero no limitándose a, computadoras; dispositivos tipo tableta; dispositivos de comunicación y organización personal, tales como puntos de acceso inalámbrico, teléfonos inteligentes o teléfonos celulares; dispositivos de videojuegos; equipo fotográfico; y dispositivos de entretenimiento, tales como reproductores de MP3 o iPods™.

L. Un *usuario* es cualquier miembro del personal de MCPS, estudiante u otro individuo autorizado para usar los sistemas de computación de MCPS. Otros individuos pueden incluir a padres, voluntarios y contratistas o personal temporal.

IV. PROCEDIMIENTOS

La siguiente sección delinea los procedimientos requeridos para ciberseguridad, protección cibernética y ética cibernética para la protección de datos e información electrónica, transacciones y firmas electrónicas, protección física, protección de sistemas y aplicaciones, protección de la red y conducta y uso. El *Manual de Procedimientos de Protección de los Sistemas de Computación de MCPS (Manual of MCPS Computer Systems Security Procedures)* explica en más detalle las responsabilidades y procedimientos específicos del usuario para la protección de los sistemas de computación y está disponible en el sitio web de MCPS.

A. Protección de Datos e Información Electrónica

Los usuarios sólo podrán acceder a información y sistemas de computación a los que ellos estén autorizados y que ellos necesiten para sus asignaciones y responsabilidades.

1. Los usuarios son responsables de sus propias cuentas individuales.

   a) Los usuarios deben cambiar sus contraseñas según se exija y deben mantener las contraseñas bajo máxima confidencialidad.

   b) Los usuarios tienen expresamente prohibido compartir sus cuentas y sus contraseñas.

   c) Cualquier violación que pueda ser rastreada al nombre de una cuenta individual será tratada como la responsabilidad del dueño de la cuenta.

2. Los usuarios deberán desconectarse de todos los sistemas antes de retirarse de una estación de trabajo o de permitir que otros la usen.

3. Es la responsabilidad de cada usuario conocer y seguir los procedimientos de seguridad, conforme a este reglamento.

4. Los usuarios deberán proteger sus datos electrónicos. (Nota: Los archivos confidenciales deberán guardarse en una ubicación segura, tal como un archivo o directorio de red de un individuo o un disco extraíble que esté luego protegido en un gabinete bajo llave.)

5. MCPS no es responsable por información que pueda perderse debido a fallas o interrupciones del sistema. Los usuarios deberán hacer copias de respaldo y asegurarse que estén archivadas en un lugar seguro.

B. Transacciones y Firmas Electrónicas

Donde las leyes del estado de Maryland, las leyes federales o las políticas o reglamentos de MCPS exijan que una transacción tenga la firma de una persona autorizada, ese requerimiento queda cumplido cuando el registro electrónico tiene una firma electrónica asociada con el mismo, usando un método aprobado de firma electrónica. Los procedimientos de autorización y uso de transacciones y firmas electrónicas están detallados en el *Manual de Procedimientos de Protección de los Sistemas de Computación de MCPS*.

C. Seguridad Física

El equipamiento de los sistemas de computación deben estar ubicados y mantenidos en un entorno físico protegido. Los usuarios son responsables de seguir las provisiones de seguridad física para las computadoras y tecnologías relacionadas.

1. Cuando los miembros del personal no estén presente para supervisar el área, todas las áreas donde se guarde valioso equipamiento de computación (incluidas las de almacenamiento permanente o temporal) deberán estar seguras.

2. No se puede retirar de una instalación de MCPS computadoras o equipamiento relacionado sin la autorización adecuada.

3. Los usuarios deben emplear procedimientos locales de responsabilidad para entregar o retirar cualquier computadora o equipamiento relacionado. Este equipamiento debe ser devuelto a la escuela, departamento, división o unidad a quien le pertenezca antes de que el usuario se retire de MCPS o transfiera a otra escuela u oficina.

4. El inventario de equipamiento local será mantenido lo más precisamente posible. El equipamiento será sumado al inventario cuando se adquiera. Los usuarios no pueden quitarle las marcas o etiquetas de inventario a las computadoras.

5. Equipamiento que se pierda o que sea robado deberá ser gestionado conforme al Reglamento EDC-RA de MCPS, *Control del Inventario de Muebles y Equipamiento*.

D. Protección de Sistemas y Aplicaciones

1. Los usuarios no deben instalar software o hardware o desactivar o modificar las configuraciones o medidas de seguridad (tales como software antivirus)

instalados en cualquier computadora u otros dispositivos digitales/electrónicos autorizados para ningún propósito sin el permiso del personal apropiado, según se expresa en el *Manual de Procedimientos de Protección de los Sistemas de Computación de MCPS*.

2. Los usuarios no deben modificar las configuraciones del sistema sin el permiso del personal apropiado, según se expresa en el *Manual de Procedimientos de Protección de los Sistemas de Computación de MCPS*.

3. Las aplicaciones y software de MCPS no pueden ser instalados o copiados a una computadora que no le pertenezca a MCPS, excepto según lo especificado por convenios de licencias.

E. Protección de la Red

Todo acceso a la red y a información de MCPS exige la aprobación de una autoridad de MCPS, autorizada en OCTO. Las cuentas o el acceso de los usuarios pueden ser retirados, suspendidos o revocados si se determina que el acceso a la red o a la información se utiliza en violación de esta o cualquier otra política o reglamento de MCPS aplicable.

F. Conducta y Uso

El uso de Internet por parte de los estudiantes y el personal será monitoreado a través de distintos métodos incluyendo, pero no limitándose a, tecnología y supervisión directa.

1. Los usuarios son responsables de asegurarse que el acceso a, o la importación de, material en redes sea para fines educativos según lo define este reglamento.

2. Cualquier material o información intencionalmente publicados o accedidos desde un sistema de MCPS o sitio web debe coincidir con el fin educativo, como lo define este reglamento.

3. Los usuarios son responsables de cumplir con las reglas aplicables al sistema o sistemas de computación que usen, incluyendo aquellos accedidos a través de Internet desde equipamientos de MCPS.

4. MCPS no tiene control sobre, y no puede ser responsable por, información que resida en otros sistemas o sitios web a los cuales haya acceso a través de MCPS. Algunos sitios y sistemas fuera de MCPS podrían contener

material difamatorio, incorrecto, abusivo, obsceno, grosero, sexualmente orientado, amenazante, racialmente ofensivo o ilegal.

5. Todo uso de las funciones de computación, redes y otros recursos tecnológicos deberá ser para fines educativos, según se define en la Sección III.D., y está sujeto a revisión por parte de MCPS, y podrá ser accedido y archivado.

6. El correo electrónico de MCPS es solamente para fines educativos. Todas las acciones están sujetas a revisión por parte de MCPS y pueden ser registradas y archivadas. Todo uso de correos electrónicos de MCPS por parte de estudiantes deberá ser autorizado para el propósito de apoyar o facilitar el proceso de aprendizaje.

7. Los estudiantes tienen prohibido el uso de correo electrónico, mensajería instantánea y salas de charla (chat) no autorizados.

8. Aunque es imposible documentar toda conducta y uso inapropiado de las funciones de computación, las siguientes pautas brindan ejemplos de infracciones de uso de computadoras y redes que están prohibidas:

   a) Alterar el sistema (también conocido como piratería (hacking)) o ayudar a otros para ocasionar alteraciones proporcionándoles instrucciones o información sobre cómo alterar cualquier sistema de MCPS (cualquier alteración no autorizada de los sistemas operativos, cuentas individuales, archivo compartido en la red, software, instalaciones de red y/u otros programas) y/o daño al equipamiento.

   b) Descifrado de contraseñas, claves de ingreso o captación no autorizada de contraseñas usando dispositivos de hardware o aplicaciones de software y/u obtener acceso o privilegios no autorizados a un nivel más elevado o intentar hacerlo.

   c) Interferir deliberadamente con el acceso de otros usuarios a la red o uso de una computadora, como a través de denegación de servicio (denial of service–DoS) o denegación de servicio distribuido (distributed denial of service–DDoS).

   d) Hacer declaraciones o tomar acciones que sean difamatorias, calumniosas o que constituyan ciberacoso, hostigamiento o intimidación de otros.

e) Intencionalmente acceder o intentar acceder a material inapropiado, según se identifica en III. H., más arriba en este documento.

f) Introducir códigos/software maliciosos, tales como virus o gusanos que causan daño o que subvierten la función prevista de los sistemas de computación de MCPS.

g) Conectar equipo no autorizado a cualquier computadora de MCPS o a la red de MCPS sin autorización de OCTO y/o su designado.

h) Usar correo electrónico para acosar o estafar a otros enviando mensajes electrónicos masivos y/o comerciales amenazantes o no solicitados a través de Internet, o usando mensajes de correo electrónico fraudulentos para obtener información personal para fines de usurpación de identidad.

i) Infiltrar las medidas de protección tecnológica, también conocidas como seguridad de la red o tecnología de filtraje, a través del uso de proxy, aplicaciones u otros métodos.

j) Borrar, falsificar, modificar, leer o copiar sin permiso el correo electrónico de otros usuarios o intentar hacerlo.

k) Leer, borrar, copiar, re-enviar, imprimir, compartir o modificar los archivos de datos de otros usuarios sin la autorización del superintendente de escuelas y/o su designado.

l) Permitir que otros usen la dirección personal de correo electrónico de MCPS, la cuenta o la contraseña de uno.

m) Permitir que otros usen la cuenta personal en la red de MCPS, los archivos de la red o la contraseña de uno.

n) Usar publicidad comercial, cartas en cadena o juegos no educativos en los sistemas de MCPS.

o) Copiar o transferir sin autorización materiales y software protegidos por derechos de autor.

p) Publicar o diseminar en Internet información de identificación personal sin autorización o publicar información falsa sobre estudiantes o empleados, usando equipamiento o recursos de MCPS.

q) Usar las redes o sistemas de computación de MCPS para beneficio personal o para cualquier actividad ilegal.

9. Se prohíbe a todos los usuarios intencionalmente participar en la divulgación, uso y diseminación no autorizada de información personal de menores.

10. Se deberá educar a los estudiantes acerca de la conducta apropiada en línea, incluyendo interacciones con otras personas en sitios de redes sociales y en salas de charla (chat) y sobre la consciencia y respuesta al ciberacoso.

11. Cualquier usuario de los sistemas de computación de MCPS que identifique un sector de Internet que contenga material inapropiado que no haya sido filtrado a través de la medida de protección tecnológica no sólo tiene el deber sino que se espera que siga los procedimientos según se detallan en el *Manual de Procedimientos de Seguridad de los Sistemas de Computación de MCPS* que está disponible en el sitio web de MCPS.

V. INCUMPLIMIENTO

A. El incumplimiento con los procedimientos y estándares expresados en este reglamento es causa adecuada para acción disciplinaria.

1. Las acciones disciplinarias para los empleados pueden incluir una conferencia, una advertencia, una carta de reprimenda, pérdida de privilegios, suspensión sin sueldo, degradación, despido y/o procesamiento penal.

2. Las acciones disciplinarias para los estudiantes pueden incluir, pero no se limitan a, una llamada telefónica a los padres o guardianes; pérdida de privilegios, restitución, suspensión y/o expulsión; y/o procesamiento penal. (Consulte el Reglamento JFA-RA de MCPS, *Derechos y Responsabilidades de los Estudiantes*, y las políticas de disciplina escolar.)

3. Las acciones disciplinarias para otros usuarios pueden incluir la pérdida de privilegios y/o procesamiento penal.

B. Cualquier usuario de los sistemas de computación de MCPS deberá reportar el uso sospechoso o inapropiado de datos, abuso del sistema de computación o posibles violaciones de seguridad. Los usuarios que están en las escuelas deberán alertar al director de la escuela o al designado del director responsable de la tecnología informática. Los usuarios que no están en las escuelas deberán alertar a sus supervisores inmediatos y al superintendente de escuelas y/o su designado. Las infracciones graves, según se estipulan en el *Manual de Procedimientos de*

Seguridad de los Sistemas de Computación de MCPS, también deberán ser reportadas a OCTO.

Historial del Reglamento: Nuevo reglamento, 22 de agosto, 1995; revisado el 13 de diciembre, 1999; nombres de las oficinas actualizados el 1ro de junio, 2000; revisado el 10 de junio, 2002; revisado el 23 de mayo, 2007; revisado el 27 de julio, 2012.