USO ACEPTABLE DE LA RED DEL DISTRITO

OBJETIVOS

Esta política establece los estándares y expectativas que rigen el uso de la Red del Distrito por parte de todos los miembros de la Junta del Distrito Escolar de la Ciudad de Rochester ("Distrito"), empleados, estudiantes, consultores, socios e invitados. La política tiene por objeto promover el uso ético, legal y relacionado con la escuela de la Red del Distrito. Todos los dispositivos electrónicos se regirán por esta política cuando dichos dispositivos estén conectados a la Red del Distrito.

RESPONSABILIDAD

El propósito de las computadoras entregadas por el Distrito, las redes cableadas y aquellas sin cables, el correo electrónico y el acceso a Internet es facilitar las comunicaciones en apoyo del trabajo legítimo del Distrito, la investigación y la educación. Para seguir siendo elegibles como usuarios, dicho uso debe apoyar los objetivos educativos y las responsabilidades de trabajo del Distrito. El acceso es un privilegio, no un derecho y el acceso conlleva responsabilidad.

DEFINICIONES

1. Red del Distrito: Todas las computadoras, redes cableadas y no cableadas, correo electrónico y teléfono, hardware, software y tecnologías relacionadas que sean propiedad o tengan licencia del Distrito, incluidas todas las redes, cableado y equipos de comunicaciones.

2. Información electrónica: Todos los correos electrónicos, archivos de audio y datos electrónicos, archivos u otros registros almacenados en la Red Distrital.

3. Fines educativos: Aquellas acciones que promuevan directamente las misiones educativas, de enseñanza, administrativas, comerciales y de servicios de apoyo del Distrito y relacionadas con cualquier instrucción, proyecto, trabajo, asignación de trabajo, tarea o función del Distrito de la que el Usuario sea responsable.

4. Materiales inapropiados: representaciones textuales, gráficas, pictóricas o auditivas de elementos que, en su conjunto y con respecto a los intereses de los estudiantes, apelan a un interés lascivo en la desnudez, el sexo o la deposición; materiales que carezcan de valor literario, artístico, político o científico serio para los estudiantes; materiales que promuevan la discriminación o el acoso contra otros por motivos de raza, religión, género, nacionalidad, orientación sexual; materiales destinados a enseñar habilidades que permitirían a un individuo participar en actividades ilegales; o materiales que violan la ley o son inconsistentes con las Políticas de la Junta de Educación, los Reglamentos del Superintendente o la misión educativa del Distrito.

5. Acceso a Internet: todos los métodos usados para conectarse a servidores y usuarios de Internet, y todos los métodos para proporcionar acceso independientemente de la financiación o las fuentes de facilitación, incluido el correo electrónico.

6. Información restringida: Cualquier dato o información para la cual la persona que accede a ella no tenga un propósito educativo. Esto también se relaciona con la información que podría considerarse pública cuando dicha información no respalde las responsabilidades del Usuario de una manera que sea beneficiosa para el Distrito y el personal.

7. Medida de protección de la tecnología: Una tecnología de filtrado de Internet que está diseñada para limitar el acceso a partes seleccionadas de Internet en función de criterios identificados. Su uso previsto en el Distrito es limitar el acceso a Material Inapropiado.

8. Equipo no autorizado: Cualquier dispositivo que no esté aprobado por el Superintendente o la persona designada para conectarse a una computadora del Distrito o a una red del Distrito, incluidos, entre otros, dispositivos de red personales como puntos de acceso inalámbricos, enrutadores de red y conmutadores de red.

9. Usuario: Cualquier miembro de la Junta de Educación, empleado del Distrito, estudiante, consultor, socio, invitado u otra persona autorizada para usar la Red del Distrito.

PROCEDIMIENTO

1. Gestión de los datos electrónicos y de la seguridad de la información

   Los usuarios sólo podrán acceder a la información y/o sistemas informáticos a los que estén autorizados y que necesiten para sus tareas y responsabilidades.

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

      i. Los usuarios deben proteger la seguridad de sus cuentas cambiando las contraseñas según las instrucciones del Departamento de Gestión y Tecnología de la Información ("IM&T") y manteniendo sus contraseñas en la más estricta confidencialidad.

      ii. Se prohíbe expresamente a los usuarios compartir cuentas y contraseñas.

      iii. Las infracciones que puedan atribuirse a un nombre de cuenta individual se considerarán responsabilidad del propietario de la cuenta.

   b. IM&T desarrollará e implementará protocolos para que las computadoras puedan bloquearse automáticamente cuando los Usuarios estén fuera de sus computadoras por un período de tiempo predeterminado. Los usuarios deben cerrar la sesión antes de permitir que otros usen su computadora.

   c. Es responsabilidad de cada usuario conocer y seguir todos los procedimientos de seguridad aplicables de acuerdo con este Reglamento.

   d. Los usuarios deben proteger sus datos electrónicos. Los archivos confidenciales deben guardarse en una ubicación segura, como la carpeta/directorio de red de una persona o un disco extraíble que luego se protege en un archivador cerrado con llave o en una ubicación segura en la nube del distrito (es decir, Google Cloud, One Drive).

   e. Los usuarios deben hacer copias de seguridad de los archivos críticos almacenados en sus computadoras y asegurarse de que las copias se almacenen en un lugar seguro.

   f. Datos e información del distrito: los empleados solo accederán a la información que; es necesario para llevar a cabo sus deberes distritales de acuerdo con el propósito previsto; es coherente con el Código de Conducta; y no califica como **Información Restringida**.

2. Seguridad Física

   Los equipos de sistemas informáticos deben ubicarse y mantenerse en un entorno físico seguro. Los usuarios son responsables de cooperar con las siguientes disposiciones de seguridad física para computadoras y tecnología relacionada.

   a. Cuando los miembros del personal no estén presentes para supervisar el área, todas las áreas (incluido el almacenamiento permanente o temporal) que alberguen equipos informáticos valiosos deben estar aseguradas.

   b. Las computadoras o equipos relacionados, excluyendo las computadoras portátiles entregadas a individuos, no pueden ser reubicados o retirados de la propiedad del Distrito sin coordinación a través del Centro de Servicio Técnico (Help Desk). Cualquier computadora o equipo relacionado solo se puede mover de un lugar a otro bajo la supervisión del Técnico de Computación del Distrito asignado a ese edificio.

   c. Los usuarios a los que se les entregue una computadora portátil deben firmar un recibo físico al tomar posesión de la computadora. La computadora portátil debe ser devuelta al Enlace de Servicios Informáticos de IM&T (ubicado en la Oficina Central) o al Técnico de la Escuela antes de que el Usuario abandone el Distrito o se transfiera a otra escuela u oficina.

   d. El Centro de Servicio Técnico (Help Desk) mantendrá una base de datos de todas las computadoras, equipos de cómputo y teléfonos celulares firmados con un recibo físico. Es responsabilidad de la persona que toma posesión del equipo y firma el recibo físico notificar al Servicio Técnico que ha devuelto el equipo para que su nombre pueda ser borrado de la base de datos como usuario en posesión del equipo.

   e. El personal del distrito debe reportar equipos perdidos y/o robados de la siguiente forma:

      i. Notificar a la policía y presentar una denuncia por robo del equipo.

         1) Obtener una copia de la denuncia policial y enviar copia a:
            a) El Director de la Oficina de Seguridad; y
            b) Oficial de Tecnología de la Información de IM&T.

         2) Completar un Formulario de Reporte de Equipo Informático Perdido, Robado o Dañado que detalle todos los artículos faltantes con su número de serie, marca, número de modelo y costos estimados. A continuación, se deben entregar copias al Director de la Oficina de Seguridad y al Oficial de Tecnología de la Información de IM&T.

3. Seguridad de sistemas y aplicaciones

   a. Los usuarios no instalarán software o hardware, ni deshabilitarán o modificarán la configuración o las medidas de seguridad (como el software antivirus) instaladas en cualquier computadora para ningún propósito sin el permiso del Centro de Servicio Técnico (Help Desk).

   b. Los usuarios no deben cambiar la configuración del sistema sin el permiso del servicio técnico de asistencia.

c. El software y las aplicaciones del Distrito no pueden ser instalados o copiados en una computadora que no sea del Distrito, excepto cuando sea autorizado por escrito por el Oficial de Tecnología de la Información.

4. Seguridad de la red

El Distrito no es responsable de la información que se encuentre en redes ajenas al Distrito, incluyendo, por ejemplo, Internet. El Distrito no tiene control sobre la información que reside en otros sistemas o sitios de Internet a los que se tiene acceso a través del Distrito. Algunos sitios y sistemas fuera del Distrito pueden contener material difamatorio, inexacto, abusivo, obsceno, profano, sexualmente orientado, amenazante, racialmente ofensivo o ilegal.

a. Los usuarios son responsables de garantizar que el acceso o la importación de material en las redes sea con fines educativos.

b. Cualquier material o información publicada o vinculada a propósito desde el sistema o sitio de Internet del Distrito debe ser consistente con el propósito educativo o comercial del Distrito, como se define en este Reglamento.

c. Los usuarios son responsables de cumplir con todas las leyes federales y estatales, las políticas de la Junta y las Regulaciones del Superintendente aplicables a los sistemas informáticos que utilizan, incluidos aquellos a los que se accede a través de Internet desde el equipo del Distrito.

d. Salvo lo dispuesto en los subpárrafos e. y f. siguientes, los equipos de propiedad personal de empleados, socios o consultores del Distrito no podrán conectarse a la Red del Distrito ni directamente a ningún equipo de propiedad del Distrito.

e. Las solicitudes de contratistas o consultores para conectar sus computadoras portátiles o de escritorio corporativas a la Red del Distrito serán consideradas y aprobadas por escrito caso por caso por el Funcionario de Tecnología de la Información o la persona designada.

f. Los contratistas aprobados deberán firmar un Formulario de Solicitud de Acceso a la Red.

g. El único acceso remoto o Red Privada Virtual ("VPN") aprobado para todos los Usuarios es a las páginas Web del Distrito a través de Internet y al sistema de correo electrónico del Distrito. El acceso remoto a todos los demás sistemas informáticos del Distrito no está permitido, salvo autorización expresa por escrito del Oficial de Tecnología de la Información.

i. El acceso VPN sólo se concede a los empleados del Distrito que utilicen equipos de sistemas informáticos basados en Windows propiedad del Distrito.

ii. Los empleados pueden solicitar acceso VPN para contratistas con una justificación comercial significativa y podría ser aprobado caso por caso por el Oficial de Tecnología de la Información o su designado. Los contratistas aprobados deberán firmar un formulario de solicitud de acceso a VPN del Distrito.

5. Conducta y uso

    a. El uso de todas las instalaciones informáticas, la Red del Distrito y otros recursos tecnológicos está destinado a Fines Educativos y está sujeto a la revisión del Distrito y puede ser registrado y archivado.

    b. El correo electrónico del Distrito es sólo para propósitos educativos del Distrito. Todos los correos electrónicos están sujetos a la revisión del Distrito y serán registrados y archivados.

        i. IM&T asignará una dirección de correo electrónico oficial del Distrito a todos los empleados. Es a esta dirección oficial a la que el Distrito enviará comunicaciones por correo electrónico a los empleados. Esta dirección de correo electrónico oficial será la que aparece en la Libreta de Direcciones Globales para el sistema de correo electrónico de Intercambio del Distrito.

        ii. Las comunicaciones a través del sistema de correo electrónico serán profesionales y apropiadas para el lugar de trabajo.

        iii. Está prohibido falsificar encabezados de correo o información de enrutamiento para ocultar los orígenes del correo o las rutas de correo.

        iv. No está permitido alterar el contenido de un mensaje atribuido a otro, salvo que los cambios se indiquen expresamente en la comunicación.

        v. El Distrito no admitirá que el correo electrónico se redirija electrónicamente a otra dirección de correo electrónico (por ejemplo, @hotmail.com, @yahoo.com, @gmail.com, etc.).

    c. Dado que las comunicaciones pueden ser críticas en cuanto al tiempo, se espera que los usuarios revisen su dirección de correo electrónico oficial de manera frecuente y constante para mantenerse al día con las comunicaciones del Distrito.

    d. Se prohíbe a todos los usuarios participar en actividades ilegales o cualquier otra actividad que de alguna manera desacredite al Distrito.

    e. Aunque es imposible identificar todas las conductas y usos inapropiados de las instalaciones informáticas, los siguientes ejemplos de infracciones de uso de computadoras y redes están expresamente prohibidos:

        i. Manipular cualquier parte de la Red del Distrito o ayudar a otros a manipular (por ejemplo, cualquier alteración no autorizada de sistemas operativos, cuentas individuales, carpetas compartidas en la red, software, instalaciones de red y/u otros programas) y/o daños al equipo.

        ii. Desencriptar contraseñas, capturar contraseñas sin autorización mediante el uso de dispositivos de hardware o aplicaciones de software, y/u obtener acceso o privilegios de nivel superior no autorizados o intentar hacerlo.

        iii. Interferir deliberadamente con el acceso a la red o el uso de la computadora por parte de otros usuarios.

iv. Usar, poseer o distribuir lenguaje, imágenes u otro material o realizar acciones que sean difamatorias, calumniosas o que acosen a otros.

v. Usar, poseer o distribuir Materiales Inapropiados.

vi. Introducir códigos como virus o gusanos informáticos que puedan causar daños o subvertir la función prevista de los sistemas informáticos del Distrito.

vii. Conectar Equipo No Autorizado a cualquier computadora del Distrito o Red del Distrito sin autorización del Superintendente o persona designada.

viii. Eludir las Medidas de Protección Tecnológica, también conocidas como seguridad de red o tecnología de filtrado.

ix. Leer, borrar, copiar, falsificar o modificar el correo electrónico de otros usuarios o intentar hacerlo.

x. Leer, borrar, copiar, reenviar, imprimir, compartir o modificar los archivos de datos de otros usuarios sin la autorización expresa y por escrito del Superintendente o de la persona designada.

xi. Permitir que otra persona utilice su dirección, cuenta o contraseña personal de correo electrónico del Distrito.

xii. Permitir que otro use su cuenta personal de la Red del Distrito, archivos de red, o contraseña.

xiii. Usar publicidad comercial, solicitaciones personales, cartas en cadena, o juegos no educativos en los sistemas del Distrito.

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

xv. Usar las redes del Distrito para publicar información personal identificable, confidencial o falsa sobre estudiantes o personal sin la debida autorización.

xvi. Usar las Redes del Distrito o sistemas de computadoras para ganancia personal o cualquier actividad ilegal o no autorizada.

xvii. Promover causas políticas o religiosas.

xviii. Distribuir datos o información confidencial del Distrito o de los estudiantes sin autorización del Superintendente o su designado.

xix. Cualquier actividad destinada a fomentar el beneficio económico personal.

xx. Cualquier propósito o acción ilegal.

f. Se prohíbe a todos los usuarios acceder o intentar acceder a sabiendas a Material Inapropiado. El uso de Internet por parte de los estudiantes y el personal se controlará mediante diversos métodos que incluyen, entre otros, la tecnología y la supervisión directa.

i. A discreción del Director de IM&T o de la persona designada, IM&T tomará medidas para bloquear o filtrar el acceso a Internet tal y como exige la Ley de Protección de Menores en Internet. Como mínimo, las siguientes categorías de sitios serán bloqueados:

1) Violencia - Esta categoría se refiere a sitios que contienen representaciones visuales o invitaciones a participar en actos violentos. Esto puede incluir guerras, crímenes, bromas, novatadas, etc. Un acto violento puede considerarse cualquier actividad que utilice la fuerza física para herir a otro ser vivo.

2) Armas/bombas - Esta categoría se refiere a cualquier sitio que promueva el uso de armas y/o bombas y la fabricación de bombas. No se incluyen los sitios relacionados con el control de armas o cuestiones sociales legítimas.

3) Temas y contenidos para adultos - Esta categoría se refiere a sitios de naturaleza adulta no definidos en otras categorías de clasificación.

4) Pornografía - Esta categoría abarca todo lo relacionado con la pornografía, incluida la pornografía suave, la pornografía blanda y la pornografía dura.

5) Fraude electrónico (Phishing) - Sitios web engañosos que pretenden engañar a los usuarios finales para que revelen datos personales como números de tarjetas de crédito, nombres de usuario de cuentas, contraseñas, números de la seguridad social, etc. Estos sitios web simulan ser los de sitios comunes y conocidos, como bancos y compañías de tarjetas de crédito.

6) Redes sociales/citas - Sitios que ofrecen servicios gratuitos o de pago que promueven la interacción, las citas u otro tipo de contactos a través de foros, chat, correo electrónico u otros métodos.

7) Intolerancia/extremismo - Esta categoría se refiere a cualquier sitio que defienda actividades militantes o el extremismo. Esto incluye grupos con opiniones políticas extremas e intolerancia hacia individuos y/o grupos basados en distinciones discriminatorias o raciales.

8) Spyware/adware - Sitios web conocidos por distribuir o contener códigos que muestran publicidad no deseada o recopilan información sobre el usuario sin su conocimiento.

9) Anonimizador - Esta categoría se refiere a sitios que permiten al usuario navegar por la red de forma anónima. También se refiere a sitios que permiten al usuario enviar correos electrónicos anónimos. También incluye sitios que brindan información o servicios de representación con omisiones.

10) Infracción de los derechos de autor - Esta categoría se refiere a sitios que ofrecen medios, software, MP3, películas en DVD o cualquier otro material protegido por derechos de autor que sea pirateado o esté

disponible ilegalmente para su compra o descarga. Esta categoría se bloquea a menudo para proteger a los propietarios de iPrism de la responsabilidad causada por la descarga e instalación de software pirateado. Tenga en cuenta que esta categoría no se refiere a sitios específicos de piratería informática.

11) Desnudos - Esta categoría se refiere a sitios que ofrecen imágenes o representaciones de desnudos. Pueden ser de forma artística o no artística, como revistas, fotografías, pinturas, esculturas, etc. Esta categoría se asignará a aquellos sitios que muestren desnudos tanto parciales como totales, aunque las imágenes no tengan carácter pornográfico.

12) Malware - Sitios web conocidos por contener código dañino que puede modificar el sistema de un usuario sin su conocimiento.

13) Denegación local - Se trata de sitios web que han sido identificados pero que no entran en ninguna de las categorías anteriores.

ii. IM&T revisará periódicamente un informe de tendencias y ajustará lo que está bloqueado o filtrado según sea necesario.

1) Se prohíbe a todos los usuarios acceder o intentar acceder a sabiendas a porciones de Internet que no promuevan los propósitos educativos, instructivos, administrativos, comerciales o de servicios de apoyo del Distrito o que no estén relacionados con cualquier instrucción, proyecto, trabajo, asignación de trabajo, tarea o función de la cual el Usuario sea responsable.

2) Cualquier usuario de la Red del Distrito que identifique una porción de Internet que contenga Material Inapropiado que no haya sido filtrado a través de la Medida de Protección Tecnológica, deberá contactar inmediatamente al servicio de asistencia técnica (Help Desk).

3) Un usuario de la Red del Distrito no utilizará esos recursos para fines comerciales personales o para ganancia financiera personal o de otro tipo.

a) El uso personal incidental de la Red del Distrito para otros fines está permitido a discreción del Superintendente o persona designada cuando el uso:

i.) no consuma injustificadamente dichos recursos;

ii.) no interfiera con el desempeño del trabajo del usuario ni con otras responsabilidades del Distrito;

iii.) no consuma una cantidad irrazonable del tiempo de trabajo del usuario;

iv.) no se refiera a temas inapropiados en un entorno escolar o laboral (por ejemplo, el acceso a sitios web pornográficos);

v.) no sea incompatible con la misión del Distrito de enseñar a los niños;

vi.) cumpla con la legislación aplicable, las políticas de la Junta de Educación y las normas del Superintendente; y

vii.) no sea **Información Restringida**.

6. Acceso a información confidencial y a otra información electrónica

   a. La información personal identificable sobre los estudiantes contenida en las comunicaciones por correo electrónico o en sus archivos adjuntos, incluida la información contenida en los expedientes académicos de los estudiantes, la información médica y la información sobre discapacidades, debe cumplir la Ley de Derechos Educativos y Privacidad de la Familia ("FERPA") y la Ley de Portabilidad y Responsabilidad del Seguro Médico ("HIPAA").

   b. Los Empleados del Distrito podrán acceder a la Información Electrónica del Distrito siempre que el empleado necesite acceder a los contenidos para desempeñar las responsabilidades de su trabajo. El acceso se limitará a la información necesaria para completar las responsabilidades del trabajo.

   c. Los Supervisores y demás personal del Distrito podrán acceder a la Información Electrónica almacenada en cualquier lugar de la Red del Distrito con el fin de revisar, conservar o eliminar todos o cualquiera de los mensajes de correo electrónico, archivos informáticos o datos electrónicos utilizados por un empleado en cualquier momento, siempre y cuando el permiso para acceder a dicha información haya sido aprobado por el Asesor Jurídico General del Distrito o su designado y el Auditor General.

   d. Para empleados de la Junta y el personal administrativo, el personal de supervisión puede acceder a la Información Electrónica almacenada en cualquier lugar de la Red del Distrito con el fin de revisar, retener o eliminar cualquiera o todos los mensajes de correo electrónico, archivos informáticos o datos electrónicos utilizados por un empleado en cualquier momento, siempre que el permiso para acceder a dicha información haya sido aprobado por el Auditor General.

   e. Todas las solicitudes de acceso a **Información Restringida** y las aprobaciones deberán estar documentadas. La solicitud debe incluir el motivo de la solicitud, el periodo de información solicitada y especificar las partes adicionales que recibirán la información. Se utilizará el Anexo 1 para documentar la solicitud.

   f. Nadie accederá ni divulgará Información del Distrito y/o **Información Restringida**, incluyendo, pero sin limitarse a, información financiera, información personal, estudiantes, padres, empleados o socios comerciales para los cuales no han sido autorizados.

g. La Oficina del Auditor General de la Junta de Educación tendrá acceso completo y sin restricciones a todos los sistemas, documentos e información dentro del Distrito Escolar de la Ciudad de Rochester.

Cualquier violación de esta política por parte de un Usuario (excepto los estudiantes del Distrito) puede resultar en la denegación de acceso y disciplina de conformidad con el acuerdo de negociación colectiva aplicable o las reglas y normas laborales de la Junta y el Superintendente, y la ley aplicable. Cualquier violación de esta política por parte de un estudiante del Distrito puede resultar en la denegación de acceso y disciplina de acuerdo con el Código de Conducta (Política 1400) y la ley aplicable.

Ref.- cruzada: Código de Conducta (1400)
Uso aceptable de la red escolar (1950-R)

Notas: Adoptada el 22 de junio de 2011 mediante Resolución No. 2010-11: 907;
Modificado el 28 de febrero de 2014 mediante la Resolución No. 2013-14: 513;
Modificado el 20 de octubre de 2022 de conformidad con la Resolución No. 2022-23: 206

ct/rp