Política del uso aceptable y de la seguridad de Internet
Implementación de la resolución del Departamento con fecha 14 de febrero de 2001
Versión revisada, a partir del 1 de julio de 2012

POLÍTICA DEL USO ACEPTABLE Y DE LA SEGURIDAD DE INTERNET

La política
El Departamento de Educación de la Ciudad de Nueva York ("**Departamento**") les proporciona acceso a los sistemas de Internet a sus empleados, agentes, alumnos y voluntarios, colectivamente conocidos como "**usuarios**" para propósitos educativos y empresariales, de conformidad con la ley vigente. Esta Política del Uso Aceptable y de la Seguridad de Internet ("**política**") gobierna toda la actividad electrónica de las personas que utilizan e ingresan a los sistemas de Internet del Departamento, incluso correo electrónico y el acceso a Internet, y se aplica al empleo de tales sistemas dentro y fuera de las instalaciones del Departamento.

Por **"sistemas de Internet del Departamento"** se entiende artefactos, conexiones a Internet (incluso inalámbricas), cuentas de correo electrónico, intranet y toda conexión remota a los sistemas mencionados. Se considera que un usuario ingresa a los sistemas de Internet del Departamento y los emplea cuando realiza actividades electrónicas en esos sistemas con cualquier artefacto, (independientemente de que el artefacto sea proporcionado por el Departamento) y de la ubicación física del usuario.

"**Artefactos proporcionados por el Departamento**" se refiere a cualquier aparato electrónico, como computadores de escritorio *(desktop)*, computadores portátiles *(laptop)*, y dispositivos portátiles, entre ellos asistentes digitales personales *(PDA)*, *e-reader*, teléfonos inteligentes, *iPad* y *tablet*.

El uso del alumnado de los sistemas de Internet del Departamento se rige por esta política, las normas, las políticas y las pautas del Departamento, los Estándares de Conducta y las Medidas Disciplinarias Uniformes para toda la Ciudad (el "**Código Disciplinario**") y la ley vigente. El uso de los empleados se rige por esta política, las regulaciones, políticas y pautas del Departamento, las políticas de empleo del Departamento, los acuerdos de contrato colectivo vigentes y las leyes vigentes.

Al emplear los sistemas de Internet del Departamento, un usuario acepta acatar esta política y todas las normas, políticas y pautas vigentes. Los usuarios deben reportarles a maestros, supervisores u otros empleados del Departamento el empleo indebido de la red o de la Internet o el recibo de toda comunicación que viole esta política.

Principios de Uso Aceptable y Seguro de Internet

General
El acceso a Internet y el correo electrónico proporcionados por el Departamento tiene como fin el fomento de la educación, la docencia, la investigación, la comunicación, la cooperación y otros propósitos relacionados con el Departamento. Los usuarios están sujetos a los mismos estándares que se esperan en un aula de clase y en un lugar de trabajo profesional.

Vigilancia y privacidad
Los usuarios no tienen derecho a privacidad cuando emplean los sistemas de Internet del Departamento. El Departamento vigila las actividades en Internet de los usuarios y se reserva el derecho a tener acceso, revisar, copiar, guardar, o borrar cualquier comunicación o archivo electrónico. Esto incluye documentos guardados en artefactos proporcionados por el Departamento, como archivos, mensajes por correo electrónico, información almacenada en computadoras *(cookies)* y registro de navegación en Internet *(Internet history)*.

El Departamento se reserva el derecho de revelar a funcionarios encargados de aplicar la ley o a terceros cualquier actividad electrónica, incluso comunicaciones, de una manera apropiada y consecuente con la ley vigente. El Departamento cooperará plenamente con funcionarios locales, estatales o federales en toda investigación legal concerniente o relacionada con actividades ilícitas llevadas a cabo a través de los sistemas de Internet.

Usos prohibidos de los sistemas de Internet del Departamento
Los usuarios no pueden participar en ninguna de las actividades prohibidas por esta política cuando empleen o ingresen a los sistemas de Internet del Departamento.

Si un usuario no está seguro de que una conducta esté prohibida, debe ponerse en contacto con un maestro, supervisor u otro empleado competente del Departamento. El Departamento se reserva el derecho de tomar medidas inmediatas en lo que guarda relación con actividades que (1) crean problemas de seguridad y protección para la entidad, estudiantes, empleados, escuelas, redes o recursos de informática, (2) usan los recursos de la institución en material carente de legítimo contenido o propósito educativo, o (3) se determina que son indebidas.

A continuación una lista no exhaustiva de ejemplos de conducta prohibida:

1. Causarle daño a otros, daños a la propiedad o a la propiedad del Departamento, como:

    a. Usar, publicar o distribuir material en lenguaje profano, indecente, vulgar, amenazante o abusivo en mensajes de correo electrónico, material publicado en páginas web del Departamento, o sitios de medios sociales profesionales;
    b. Ingresar, usar, publicar o distribuir información o material pornográfico o de otra manera obsceno, promover actos ilegales o peligrosos, o fomentar violencia o discriminación. Si los usuarios, sin darse cuenta, tienen acceso a tal información, deben inmediatamente revelar el acceso inadvertido de una manera especificada por la escuela o la oficina de la división central;
    c. Tener acceso, publicar o distribuir material agravante, discriminatorio, incendiario, u odioso, o hacer declaraciones perjudiciales o falsas acerca de otros;
    d. Enviar, publicar o de otra manera distribuir cadenas de cartas o participar en la divulgación de material no solicitado o basura *(spamming)*;
    e. Dañar equipo de computación, archivos, datos o el Sistema de Internet del Departamento, de cualquier manera, incluso propagar virus informáticos, vandalizar datos, *software* o equipo, causar daños o inutilizar la propiedad electrónica de otros, o participar en conducta que podría interferir o producir un riesgo de interrupción del entorno educativo o de trabajo del Departamento;
    f. Utilizar el Sistema de Internet del Departamento de un modo que interfiera la educación del usuario o de otras personas o los deberes laborales del usuario o terceros;
    g. Descargar, publicar, reproducir o distribuir música, fotografías, videos u otros trabajos en violación de leyes vigentes de propiedad intelectual. Música, fotografías y videos deben ser descargados sólo para propósitos del Departamento y no para actividades personales. Si un trabajo especifica cómo se debe emplear tal trabajo, el usuario debe seguir los requisitos manifestados. Si los usuarios no están seguros de que puedan emplear un trabajo, deben solicitar el permiso del dueño de la propiedad intelectual o de la marca registrada;
    h. Participación en plagio. El plagio es tomar las ideas o los trabajos escritos de otros y presentarlos como si fueran originales del usuario.

2. Obtener o tratar de obtener acceso no autorizado a los sistemas de Internet del Departamento, o al sistema de computación de terceros, como:

    a. Maliciosas actividades de alteración *(tampering)*, suplantación de identidad *(phishing)* o pirateo *(hacking)*;
    b. Búsqueda intencionalmente de contraseñas pertenecientes a otros usuarios;
    c. Revelación a otras personas de la contraseña de un usuario en los sistemas de Internet del Departamento. Sin embargo, los estudiantes pueden compartir con sus padres sus contraseñas en el Departamento;
    d. Modificación de las contraseñas pertenecientes a otros usuarios;
    e. Intento de ingresar al sistema a través de la cuenta de otra persona;
    f. Intento de obtener acceso al material que el Departamento haya bloqueado o filtrado;
    g. Ingresar, copiar, o modificar sin autorización los archivos de otro usuario;
    h. Disfraz de la identidad de un usuario;
    i. Uso de la contraseña o el identificador de una cuenta no perteneciente al usuario; o
    j. Participación en usos que posibilitan el acceso a las cuentas de otras personas u otras redes de informática.

3. Utilizar los sistemas de Internet del Departamento para fines comerciales, como:

Department of Education

a. Empleo de los sistemas de Internet del Departamento para beneficio financiero personal;
b. Realización de actividades de lucro, de publicidad personal u otro tipo de comunicaciones no relacionadas con el trabajo del Departamento;
c. Participación en actividades de recaudación de fondos (excepto como lo establece la Disposición A-610 del Canciller); o
d. Utilización de los sistemas de Internet del Departamento en nombre de un funcionario electo, candidato, candidatos, lista de candidatos o una organización o comité de tipo político;

4. Participación en actividades delictivas u otras actividades ilícitas.

Filtración

En concordancia con la Ley de Protección a los Niños en Internet ***("CIPA")***, el Departamento bloquea o filtra el contenido de Internet considerado impropio para menores. Esto incluye pornografía, material obsceno, y otro material que puede ser peligroso para los menores. El Departamento también puede bloquear o filtrar otro material considerado inapropiado, carente de contenido educativo, no relacionado con el trabajo o que constituya una amenaza para la red. El Departamento puede, a su discreción, desactivar el filtro para ciertos usuarios que hagan investigaciones auténticas o de buena fe, o para otros propósitos legales educativos o de trabajo.

Los usuarios no pueden usar ningún sitio web, ni aplicación ni métodos para eludir filtros de la red, ni realizar otras actividades ilegales.

Para información adicional concerniente a la *CIPA* consulte el siguiente enlace:

http://www.fcc.gov/guides/childrens-internet-protection-act

Protección de información confidencial de identificación personal

La Ley de Privacidad y Derechos Educativos de la Familia ***("FERPA")*** les prohíbe a funcionarios escolares del Departamento revelar a terceros sin el consentimiento de los padres de familia información de identificación personal ***("PII")*** contenida en los registros de los alumnos y las familias. Sin embargo, se pueden aplicar varias excepciones a esta regla general.

Todos los usuarios de los sistemas de Internet del Departamento deben cumplir con *FERPA* y la Disposición A-820 del Canciller, Confidencialidad y Divulgación de Registros Estudiantiles; Retención de Registros. Si no está seguro de que la actividad cumple con *FERPA* o la Disposición A-820 del Canciller, comuníquese con el funcionario en jefe a cargo de seguridad de la información.

Las comunicaciones internas con un abogado del Departamento también pueden ser confidenciales. En consecuencia, los usuarios no deben enviar ni distribuir tales comunicaciones, sin consultar primero con el abogado. Los usuarios deben asegurarse de que los mensajes de correo electrónico que incluyan o anexen información confidencial se envíen sólo a los destinatarios previstos.

Seguridad en Internet para los estudiantes

1. Responsabilidades del Departamento:

a. El Departamento impartirá un plan de estudios acerca de conducta apropiada en Internet, lo cual incluye relacionarse con otras personas en redes sociales y en salas de conversación, y toma de conciencia sobre acoso cibernético y respuesta a ese acoso.

b. El Departamento trabajará para mantener la protección y la seguridad de menores cuando utilicen correo electrónico, salas de conversación y otras formas de comunicaciones electrónicas directas.

c. En la medida en que sea apropiado, el Departamento les proporcionará a los estudiantes, los empleados y los padres de familia pautas e instrucciones para la seguridad del alumnado cuando utilice Internet.

2. Uso de los sistemas de Internet del Departamento por parte de los estudiantes

   a. Los alumnos no deben revelar información sobre ellos mismos ni otras personas ni en redes sociales, ni en salas de conversación, ni en mensajes por correo electrónico ni en otras comunicaciones electrónicas directas, ni en ningún otro foro de Internet. Por ejemplo, los educandos no deben revelar su domicilio ni sus números telefónicos fijos ni celulares. Tampoco deben exhibir fotos de ellos mismos, ni imágenes de otras personas.

   b. No deben reunirse físicamente con personas que ellos hayan conocido sólo a través de Internet.

   c. Los estudiantes deben revelar pronto a sus maestros u otros empleados de la escuela los mensajes u otra actividad recibida que sea indebida o los haga sentirse incómodos.

   d. Tampoco deben guardar sus contraseñas en los computadores del Departamento.

3. Uso por parte de los maestros de los sistemas de Internet del Departamento, incluso redes sociales, para actividades de clase

   a. Los maestros deben educar a sus alumnos acerca de conducta apropiada en Internet, lo cual incluye relacionarse con otras personas en redes sociales y en salas de conversación, y toma de conciencia sobre acoso cibernético y respuesta a ese acoso. Los docentes deben consultar la Guía del Departamento para la Ciudadanía en la Era Digital, y otros recursos educativos gratuitos sobre seguridad cibernética disponibles en Internet.

   b. Las redes sociales

      - Los "**medios sociales**" se definen como cualquier forma de publicación o plataforma por Internet que permite la comunicación interactiva, incluso redes sociales, *blogs*, sitios de Internet, foros de Internet, y *wikis*. Como ejemplos de redes sociales podemos citar a *Facebook*, *Twitter*, *YouTube*, *Google+*, y *Flickr*.
      - Las escuelas usan una variedad de tecnologías de comunicación interactiva por Internet para mejorar la enseñanza y el aprendizaje del alumnado. Las redes sociales se deben emplear sólo con fines educativos escolares relacionados con lecciones y tareas y para facilitar la comunicación entre maestros y estudiantes.
      - El Departamento limita el acceso a esas redes a personas dentro de la institución y a funcionarios escolares. Se requiere la autorización de los padres en caso de que el acceso a una red social se extienda más allá de personas dentro del Departamento y funcionarios escolares.
      - Si las actividades de Internet incluyen redes sociales, los maestros deben remitirse a las Pautas de Redes Sociales, las cuales están incorporadas en esta política.

4. Padres:

   a. Aun cuando los estudiantes generalmente estarán sometidos a supervisión cuando utilicen el Sistema de Internet del Departamento en instalaciones escolares, no es factible para la institución vigilar y aplicar una amplia gama de valores sociales en el uso de Internet por parte del alumnado. Los padres son fundamentalmente los responsables de inculcarles a sus hijos este conjunto particular de valores familiares, y explicarles cuál material es aceptable y cuál no es aceptable para buscarlo en los sistemas de Internet del Departamento.

   b. Los padres son exclusivamente responsables de vigilar el uso de Internet por parte de sus hijos cuando los niños obtienen acceso a los sistemas de Internet del Departamento desde el hogar o desde un sitio que no sea la escuela. El Departamento puede emplear o no emplear sus sistemas de filtración para limitar el acceso desde el hogar a los sistemas de Internet. Los padres deben consultar con la escuela o el Departamento.

Violaciones a esta política
El Departamento, incluso las oficinas centrales y las escuelas, se reservan el derecho de cancelarle en cualquier momento el acceso a cualquier usuario a los sistemas de Internet, entre ellos el correo electrónico.

Si un estudiante quebranta esta política, se tomarán medidas punitivas apropiadas de conformidad con el Código Disciplinario y las disposiciones del Canciller. Si a un estudiante le revocan el acceso al Sistema de Internet del Departamento, no puede ser penalizado académicamente, y la institución se cerciorará de que el alumno continúe teniendo una oportunidad significativa de participar en el programa educativo.

Las violaciones de los empleados a esta política se manejarán mediante la disciplina correspondiente.

Todos los usuarios deben revelar pronto a su maestro, supervisor, director o administrador toda información recibida que sea indebida o los haga sentirse incómodos.

Limitación de la responsabilidad
El Departamento no otorga ninguna garantía acerca de la calidad de los servicios que proporciona y no se responsabiliza por reclamos, pérdidas, daños, costos u otras obligaciones resultantes del uso de la red o las cuentas. Todo cargo adicional que declare un usuario como resultado del empleo de la red del Departamento corre por cuenta del usuario. El Departamento también niega toda responsabilidad por la precisión o la calidad de la información obtenida a través del acceso de los usuarios al sistema. Toda declaración, accesible en la red de un computador o en Internet, se considera que es el punto de vista individual del autor y no el punto de vista del Departamento, sus afiliados o sus empleados.

Copias de esta política y preguntas
El Departamento se reserva el derecho de enmendar y revisar esta política en todo momento conforme se haga necesario. Esta política está disponible a petición de parte interesada y en el sitio web del Departamento: http://schools.nyc.gov/Offices/EnterpriseOperations/DIIT/WebServices/iaup/default.htm#preamble.

Inquietudes relacionadas con esta disposición deberán dirigirse a:

NYC Department of Education
Office of Communications & Media Relations
52 Chambers Street, Room 314
New York, NY 10007
Teléfono: 212-374-5141
Fax: 212-374-5584