

Descriptor Term:
TECHNOLOGY ACCEPTABLE USE AND INTERNET SAFETY --
STUDENTS

Descriptor Code:
3.6140

Legal References: U.S. Const. amend. I; Children's Internet Protection Act, 47 U.S.C. 254(h)(5); Electronic Communications Privacy Act, 18 U.S.C. 2510-2522; Family Educational Rights and Privacy Act, 20 U.S.C. 1232g; 17 U.S.C. 101 *et seq.*; 20 U.S.C. 6777; G.S. 115C-325(e), -391

Cross References:

In the 21st Century, technology tools and electronic resources are an integral part of a comprehensive educational program. Through these, both students and staff are able to extend classrooms beyond the four walls of their schools, enriching experiences and communicating on a global level.

Computers, other electronic devices, programs, networks and the Internet support instruction, appeal to different learning styles and meet the educational goals of the board.

Use of technological resources should be integrated and infused into the system's educational program. Technological resources should be used in teaching the North Carolina Standard Course of Study and in incorporating national curriculum standards. They should also be an integral part of a comprehensive system communication program, facilitating exchange of information.

It is the policy of the board to:

1. prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications;
2. prevent unauthorized access and other unlawful online activity;
3. prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and
4. comply with the Children's Internet Protection Act [Pub. L. No. 106-544 and 47 USC 254(h)].

The superintendent shall ensure that school system computers with Internet access comply with federal requirements regarding filtering software, Internet monitoring and Internet safety policies. The superintendent shall develop any regulations and submit any certifications necessary to meet such requirements.

A. REQUIREMENTS FOR USE OF TECHNOLOGICAL RESOURCES

The use of school system technological resources, such as computers and other electronic devices, networks, and the Internet, is a privilege, not a right. Before using the Internet, all students must be trained about appropriate on-line behavior. Such training must cover topics such as cyberbullying and interacting with others on social networking websites and in chat rooms.

Anyone who uses school system computers or electronic devices or who accesses the school network or the Internet at an educational site must comply with the requirements listed below. Before using school system technological resources, students must sign a statement indicating that they understand and will strictly comply with these requirements. Failure to adhere to these requirements will result in disciplinary action, including revocation of user privileges. Willful misuses may result in disciplinary action and/or criminal prosecution under applicable state and federal law.

1. School system technological resources are provided for school-related purposes only. Acceptable uses of such technological resources are limited to activities that support learning and teaching. Use of school system technological resources for commercial gain or profit is prohibited.
2. Under no circumstance may software purchased by the school system be copied for personal use.
3. Students and must comply with all applicable board policies, administrative regulations, and school standards and rules in using technological resources. All applicable laws, including those relating to copyrights and trademarks, confidential information, and public records, apply to technological resource use. Any use that violates state or federal law is strictly prohibited.
4. No user of technological resources, including a person sending or receiving electronic communications, may engage in creating, intentionally accessing, downloading, storing, printing or transmitting images, graphics (including still or moving pictures), sound files, text files, documents, messages or other material that is obscene, defamatory, profane, pornographic, harassing or considered to be harmful to minors.
5. Users of technological resources may not send electronic communications fraudulently (i.e., by misrepresenting the identity of the sender).
6. Users must respect the privacy of others. When using e-mail, chat rooms, blogs or other forms of electronic communication, students must not reveal personally identifiable, private or confidential information, such as the home address or telephone number, of themselves or fellow students. In addition, school employees must not disclose on the Internet or on school system websites or web pages any personally identifiable information concerning students (including names, addresses or pictures) without the written permission of a parent or guardian or an eligible student, except as otherwise permitted by the Family Educational Rights and Privacy Act (FERPA) or policy 4.8000 Student Records. Users also may not forward or post personal communications without the author's prior consent.
7. Users are prohibited from cyberbullying and other harassing activities conducted through school networks.

Harassment includes, but is not limited to, slurs, comments, jokes, innuendoes, unwelcome compliments, cartoons, visual depictions, pranks, or verbal conduct relating to an individual that (a) have the purpose or effect of creating an intimidating, hostile or offensive environment; (b) have the purpose or effect of unreasonable interfering with an individual's work or school performance; or (c) interfere with school operations.
8. Users who intentionally or negligently damage computers, computer systems, electronic devices, software or computer networks are guilty of vandalism. Users may not knowingly or negligently transmit computer viruses or self-replicating messages or deliberately try to degrade or disrupt system performance. Users must scan any downloaded files for viruses.
9. Users may not create or introduce games, network communications programs or any foreign program or software onto any school system computer, electronic device or network without the express permission of the chief technology officer or designee.

10. Users are prohibited from engaging in unauthorized or unlawful activities, such as “hacking” or using the computer network to gain or attempt to gain unauthorized or unlawful access to other computers, computer systems or accounts. Unauthorized disclosure, use, and dissemination of personal identification information regarding minors is forbidden by the Children’s Internet Protection Act.
11. Users are prohibited from using another individual’s computer account. Users may not read, alter, change, execute or delete files belonging to another user without the owner’s express prior permission.
12. Users are prohibited from connecting any personal technologies to system owned and maintained local, wide, or metro area networks without permission of the board. These include computers, wireless access points and routers, printers, iPods, smartphones, PDAs.
13. If a user identifies a security problem on a technological resource, he or she must immediately notify a system administrator. Users must not demonstrate the problem to other users. Any user identified as a security risk will be denied access.
14. It is the responsibility of school administrators and staff to supervise student use of the internet during instructional time as well as enforcing this policy.
15. Views may be expressed as representing the view of the school system or part of the school system only with prior approval by the superintendent or designee.
16. While the board undertakes comprehensive security measures, appropriate use of school networks and the Internet ultimately remains the responsibility of the user. Therefore, the board is not responsible for loss of or corrupted data, service interruptions or delays, obtaining information of poor quality, or other inaccurate information.

B. Restricted Material on the Internet

Before a student may use the Internet for any purpose, the student’s parent must be made aware of the possibility that the student could obtain access to inappropriate material. The parent and student must sign a consent form acknowledging that the student user is responsible for appropriate use of the Internet and consenting to monitoring by school system personnel of the student’s e-mail communication and use of the Internet.

The board is aware that there is information on the Internet that is not related to the educational program. The board also is aware that the Internet may provide information and opportunities to communicate on subjects that are not suitable for school-age children and that many parents would find objectionable. The benefits from the valuable information and interaction available to students, however, outweigh the disadvantages of the possibility that students may find inappropriate material. School system personnel shall take reasonable precautions to prevent students from having access to inappropriate materials, such as violence, nudity, obscenity or graphic language that does not serve a legitimate pedagogical purpose. The superintendent shall ensure that the Internet service provider or technology personnel have installed a technology protection measure that blocks or filters Internet access to audio or visual depictions that are obscene, that are considered pornography or that are harmful to minors. School officials may disable such filters for an adult who uses a school-owned computer for bona fide research or another lawful educational purpose. School system personnel may not restrict Internet access to ideas, perspectives or viewpoints if the restriction is motivated solely by disapproval of the ideas involved.

C. PRIVACY

No right of privacy exists in the use of technological resources. School system administrators or individuals designated by the superintendent may review files, monitor all communication, and intercept e-mail messages to maintain system integrity and to ensure compliance with board policy and applicable laws and regulations. School system personnel shall monitor on-line activities of individuals who access the Internet via a school-owned computer.

D. PERSONAL WEBSITES

The superintendent may use any means available to request the removal of personal websites that substantially disrupt the school environment or that utilize school system or individual school names, logos or trademarks without permission.

Though school personnel generally do not monitor students' Internet activity conducted on non-school system computers during non-school hours, when a student's on-line behavior has a direct and immediate effect on school safety or maintaining order and discipline in the schools, the student may be disciplined in accordance with policy 4.3600 Code of Student Conduct.

E. Disciplinary action

Disciplinary action for students who violate this policy shall be consistent with the policy 4.3600 Code of Student Conduct.

REVISADO 24 DE MAYO, 2010

Término Descriptivo:
TECNOLOGÍA USO ACEPTABLE Y SEGURIDAD EN INTERNET --
ESTUDIANTES

Código Descriptivo:
3.6140

Referencias Legales: Enmienda de la Const. de los E.U.; Ley de Protección de los Niños en Internet, 47 U.S.C. 254(h)(5); Acto de Privacidad en las Comunicaciones Electrónicas, 18 U.S.C. 2510-2522; Derechos Educativos de la Familia y Ley de Privacidad, 20 U.S.C. 1232g; 17 U.S.C. 101 *et seq.*; 20 U.S.C. 6777; G.S. 115C-325(e), -391

Referencias Cruzadas:

En el siglo XXI, las herramientas tecnológicas y los recursos electrónicos son una parte integral de los programas educativos reglados. A través de éstos, tanto los estudiantes como el profesorado pueden extender el ámbito académico más allá del recinto escolar, enriquecerse con nuevas experiencias y comunicarse a nivel global.

Las computadoras, otros aparatos electrónicos, programas, redes y la enseñanza de apoyo vía Internet atraen diferentes estilos de aprendizaje y ayudan a cumplir los objetivos educacionales de la junta educativa.

El uso de los recursos tecnológicos debe estar integrado e incluido en el programa educativo de cada sistema escolar. Los recursos tecnológicos se deben utilizar para enseñar el Programa General de Estudios de Carolina del Norte y en incorporar los requisitos del currículo nacional. También deberían ser parte integrante de un programa general de comunicación de sistemas que facilite el intercambio de información.

Es política de la junta:

1. prevenir el acceso del usuario de su red informática a material inapropiado de Internet, correo electrónico u otras formas de comunicación electrónica también, así como su transmisión;
2. prevenir el acceso no autorizado y otras actividades ilegales en línea;
3. prevenir la revelación, uso o propagación no autorizada en línea de información identificativa personal de menores; y
4. cumplir con el Acta de Protección Infantil en Internet (Children's Internet Protection Act) [Pub. L. No. 106-544 and 47 USC 254(h)].

El superintendente se asegurará de que las computadoras del sistema escolar con acceso a Internet cumplen con los requisitos federales sobre filtración de software, supervisión de Internet y las normas de seguridad en Internet. El superintendente desarrollará toda la regulación y someterá todos los certificados necesarios para cumplir dichos requisitos.

B. REQUISITOS PARA EL USO DE LOS RECURSOS TECNOLÓGICOS

El uso de los recursos tecnológicos del sistema escolar, como computadoras y otros aparatos electrónicos, redes de comunicación e Internet, es un privilegio y no un derecho. Antes de utilizar Internet, todos los alumnos deben recibir formación sobre el comportamiento adecuado en línea.

Dicha formación debe cubrir tópicos como acoso cibernético e interacción con otros en sitios web de actividad social y chateo.

Todo el que use las computadoras o los aparatos electrónicos del sistema escolar o que accede a la red escolar o a Internet en una instalación educativa deberá cumplir los requisitos listados a continuación. Antes de utilizar los recursos tecnológicos del sistema escolar, los estudiantes

tienen que firmar una declaración que indique que comprenden y que cumplirán escrupulosamente con dichos requisitos. En caso de no adherirse a tales requisitos, recibirán un correctivo disciplinario, que puede incluir la revocación de sus privilegios de usuario. El mal uso intencionado puede resultar en correctivo disciplinario y/o acción legal bajo las leyes estatales y federales en vigor.

- 1) Los recursos tecnológicos del sistema escolar sólo están disponibles para su uso con propósitos escolares. Los usos aceptables de dichos recursos tecnológicos se limitan a las actividades que apoyen la enseñanza y el aprendizaje. Está prohibido el uso de los recursos tecnológicos del sistema escolar para ganancia o beneficio de índole comercial.
- 2) No se podrá bajo ninguna circunstancia copiar software adquirido por el sistema escolar para uso personal.
- 3) Los estudiantes tienen que cumplir todas las directivas en vigor de la junta educativa, regulaciones administrativas y reglas y normas escolares de uso de los recursos tecnológicos. Todas las leyes en vigor, incluyendo aquéllas relativas a derechos de autor y marcas comerciales registradas, información confidencial y archivos de datos públicos se aplican al uso de los recursos tecnológicos. Está estrictamente prohibido cualquier uso que viole las leyes estatales y federales.
- 4) Ningún usuario de los recursos tecnológicos, incluyendo personas que envíen o reciban comunicación electrónica, podrá crear, acceder intencionadamente, descargar, almacenar, imprimir o transmitir imágenes, gráficos (incluyendo fotografía fija o en movimiento), archivos de sonido, archivos de texto, documentos, mensajes u otro material de índole obscena, difamatoria, profana, pornográfica, amenazadora o considerada perjudicial para menores.
- 5) Los usuarios de los recursos tecnológicos no podrán enviar comunicaciones electrónicas de forma fraudulenta (i.e., falsificando/utilizando indebidamente la identidad del remitente).
- 6) Los usuarios deben respetar la privacidad ajena. Cuando utilicen correo electrónico, espacios de chateo, blogs u otras formas de comunicación electrónica, los estudiantes no pueden ni deben revelar ninguna información personal identificativa, privada o confidencial, tal como el domicilio o número de teléfono, suya o de otros estudiantes. Además, el personal escolar no puede ni debe publicar en Internet o en sitios web o páginas web del sistema escolar ninguna información que identifique personalmente a los estudiantes, incluyendo nombres, direcciones o fotografías sin la autorización por escrito del padre, madre, tutor o estudiante legalmente capacitado, excepto como esté permitido por el Acta de Derechos Educativos y de Privacidad de la Familia (FERPA) o el reglamento 4.8000 sobre Información del Estudiante. Los usuarios tampoco pueden reenviar, enviar o publicar comunicaciones personales sin el previo consentimiento del autor.
- 7) Se prohíbe a todos los usuarios el acoso cibernético u otras actividades de acoso llevadas a cabo a través de las redes informáticas escolares.
 - i. El acoso incluye, pero no se limita a, comentarios, chistes, insinuaciones, indirectas, cumplidos no deseados, tiras cómicas, representaciones visuales, bromas o comportamientos verbales sobre un individuo (a) con el propósito o efecto de crear un entorno intimidatorio, hostil u ofensivo; (b) con el propósito o efecto de interferir sin razón con el trabajo o rendimiento académico; o (c) interferir con las operaciones escolares.
- 8) Los usuarios que intencionalmente o por negligencia dañen computadoras, sistemas de computación, aparatos electrónicos, software o redes informáticas son culpables de vandalismo.

Los usuarios no pueden ni deben con conocimiento o por negligencia transmitir virus informáticos o mensajes de autorespuesta, o intentar degradar o distorsionar deliberadamente el funcionamiento del sistema. Los usuarios deben escanear todos los archivos instalados para detectar virus.

- 9) Los usuarios no pueden ni deben crear o introducir juegos, programas de comunicación de redes o cualquier programa o software extraño en ninguna computadora, aparato electrónico o red informática del sistema escolar sin el expreso permiso del encargado jefe de tecnología o su designado.
- 10) Se prohíbe a los usuarios participar en actividades no autorizadas o ilegales, como “hacking”, o utilizar la red informática para conseguir o intentar conseguir acceso no autorizado o ilegal a otras computadoras, o sistemas o cuentas de computadoras. El Acta de Protección a los Niños en Internet (Children’s Internet Protection Act) prohíbe la revelación, uso y publicación no autorizada de información identificativa personal de menores.
- 11) Se prohíbe a los usuarios utilizar las cuentas de computadora de otras personas. Los usuarios no pueden ni deben leer, alterar, cambiar, ejecutar o borrar ficheros que pertenezcan a otro usuario sin el expreso permiso previo de su dueño.
- 12) Se prohíbe a los usuarios conectar ningún aparato personal de tecnología a las redes informáticas propiedad del sistema escolar y mantenidas por el área local, externa o metropolitana sin permiso de la junta educativa. Éstas incluyen computadoras, puntos y enrutadores de acceso inalámbrico, impresoras, iPods, teléfonos inteligentes y asistentes digitales personales (PDAs).
- 13) Si un usuario identifica un problema de seguridad o un recurso tecnológico, debe notificar inmediatamente a un administrador del sistema. Los usuarios no deben mostrar el problema a otros usuarios. Se denegará el acceso a cualquier usuario identificado como riesgo a la seguridad.
- 14) Es responsabilidad de los administradores y personal escolar controlar el uso de Internet por parte de los estudiantes durante las horas lectivas, así como la aplicación y refuerzo de esta orden administrativa.
- 15) Sólo se pueden expresar los puntos de vista como pertenecientes a todo o parte del sistema escolar previa aprobación del superintendente o su designado.
- 16) Aunque la junta educativa es la encargada de llevar a cabo las medidas generales de seguridad, el uso apropiado de Internet y de las redes escolares de informática es responsabilidad del usuario. Por tanto, la junta no es responsable de la pérdida o corrupción de datos, interrupciones o retrasos del servicio, obtención de información de baja calidad u otra información inexacta.

F. Material Restringido en Internet

Antes de que un estudiante pueda utilizar Internet con cualquier propósito, su padre o madre deben ser debidamente informados de la posibilidad de que el estudiante pueda obtener acceso a material inapropiado. El padre o madre y el estudiante deben firmar un formulario de consentimiento reconociendo que el estudiante usuario es responsable del uso apropiado de Internet y consintiendo el control por parte del personal del sistema escolar de las comunicaciones del estudiante por correo electrónico y su uso de Internet.

La junta educativa es consciente de la existencia en Internet de información no relacionada con el programa educativo. Asimismo, también es consciente de que Internet puede proporcionar

información y oportunidades de comunicación que no son apropiadas para niños en edad escolar y a las que muchos padres considerarían no recomendables. No obstante, los valiosos beneficios que proporcionan la información y la interacción disponibles para los estudiantes superan con mucho la desventaja de la posibilidad de que éstos puedan encontrar material inapropiado. El personal del sistema escolar tomará las precauciones razonables para prevenir el acceso de los estudiantes a material inapropiado relativo a violencia, desnudez, obscenidades o lenguaje gráfico que no sirva a un propósito pedagógico legítimo. El superintendente se asegurará de que el proveedor de servicio de Internet o el personal de tecnología hayan instalado una medida de protección tecnológica que bloquee o filtre el acceso a imágenes de audio o video de naturaleza obscena, consideradas de índole pornográfica o perjudiciales para menores. Dichos filtros pueden ser desactivados por un empleado de las escuelas en el caso de un adulto que utilice una computadora propiedad de la escuela con fines auténticos de investigación u otro propósito educativo legal. El personal del sistema escolar puede no restringir el acceso a Internet de ideas, perspectivas o puntos de vista si la restricción está solamente motivada por la desaprobación de dichas ideas.

G. PRIVACIDAD

No existe ningún derecho de privacidad en el uso de recursos tecnológicos. Los administradores o individuos pertenecientes al sistema escolar designados por el superintendente pueden revisar ficheros, controlar todas las comunicaciones e interceptar correos electrónicos para mantener la integridad del sistema y para asegurarse del cumplimiento con el reglamento de la junta educativa y las reglas y leyes aplicables en vigor. El personal del sistema escolar controlará las actividades en línea de los individuos que accedan a Internet a través de una computadora propiedad del sistema escolar.

H. SITIOS WEB PERSONALES

El superintendente puede utilizar cualquier medio a su disposición para solicitar la eliminación de sitios web personales que alteren significativamente el entorno escolar o que utilicen los nombres del sistema escolar o escuelas individuales, logotipos o marcas comerciales sin permiso.

Aunque el personal escolar generalmente no controla la actividad en Internet de los estudiantes que se lleva a cabo en computadoras no pertenecientes al sistema escolar durante horas no lectivas, cuando el comportamiento en línea de un estudiante tiene un efecto directo e inmediato en la seguridad escolar o en mantener el orden y la disciplina en las escuelas, el estudiante puede recibir un correctivo de acuerdo con el reglamento 4.3600 del Código de Conducta del Estudiante.

I. MEDIDAS DISCIPLINARIAS

Las medidas disciplinarias para los estudiantes que violen este reglamento serán de acuerdo con el reglamento 4.3600 del Código de Conducta del Estudiante.

Please fill in the form below and return the form to the school.

Catawba County Schools Acceptable Use and Internet Safety Policy for Students
Board Policy 3.6140

Student Agreement:

I understand and will abide by the above Catawba County Schools Acceptable Use and Internet Safety Policy. I further understand that any violation will result in the loss of access privileges, school disciplinary action, and possible criminal prosecution.

Student Name (please print) _____

Student Signature: _____ Date: _____

School: _____

Expected Year of Graduation _____ Home Room Teacher _____

Parent or Guardian Agreement:

I have read the above Catawba County Schools Acceptable Use and Internet Safety Policy. I understand that this access is designed for educational purposes only. I also recognize, while Catawba County Schools maintains a firewall and filtering software, it is impossible for the filtering and blocking technology to block access to all inappropriate materials. However, I accept full responsibility for my child's compliance with the above Rules and Regulations and, hereby, give my permission for my child to use Catawba County Schools' Networks.

Parent or Guardian Name (please print): _____

Parent /Guardian Signature: _____ Date: _____

This agreement will remain in effect as long as the student is enrolled in the school listed above, or until the parent submits a letter revoking permission for the student to use the CCS networks.

Favor de completar este impreso y regresarlo a la escuela.

Escuelas del Condado de Catawba - Uso Aceptable y Normativa de Seguridad en Internet
para los Estudiantes
Reglamento de la Junta Educativa 3.6140

Acuerdo para el Estudiante:

Comprendo y me comprometo a cumplir este Uso Aceptable y Normativa de Seguridad en Internet para los Estudiantes de las Escuelas del Condado de Catawba. Comprendo además que toda violación de esta normativa resultará en pérdida de privilegios de acceso, medida disciplinaria escolar y posible acción policial.

Nombre del Estudiante (en mayúsculas) _____

Firma del Estudiante: _____ Fecha: _____

Escuela: _____

Año de Graduación Previsto _____ Maestro/a Principal _____

Acuerdo para Padres y Tutores:

He leído este Uso Aceptable y Normativa de Seguridad en Internet para los Estudiantes de las Escuelas del Condado de Catawba. Comprendo que este acceso tiene sólo propósitos educativos. También soy consciente de que, aunque las Escuelas del Condado de Catawba mantienen un cortafuegos (firewall) y software de filtrado, es imposible para la tecnología de filtrado y bloqueo bloquear el acceso a todos los materiales inapropiados e indebidos. De cualquier manera, acepto toda responsabilidad del cumplimiento de las Normas y Reglamentos arriba indicados por parte de mi hijo/a. Por tanto, doy permiso a mi hijo/a para que utilice la red informática de las Escuelas del Condado de Catawba.

Nombre del padre/madre/tutor (en mayúsculas): _____

Firma del padre/madre/tutor: _____ Fecha: _____

Este acuerdo permanecerá vigente mientras el estudiante permanezca inscrito en la escuela mencionada arriba, o hasta que el padre/madre envíen una carta que revoque el permiso del estudiante para utilizar la red de CCS.