Rules for Internet Acceptable Use

Implementing Department Resolution of February 14, 2001
Revised as of February 14, 2006

Index

PREAMBLE

The basic principles that animate the Internet Acceptable Use Policy that follows is to:

- make powerful new Internet resources, especially broadband access, widely and equitably available and affordable for all learners;
- provide continuous and relevant training and support for educators and administrators;
- build a new research framework of how people learn in the Internet age; and
- develop high quality online educational content that meets the highest standards of educational excellence.

It is intended that Internet access will improve the processes of teaching and learning as well as facilitate improvements in communication between all members of the learning community, especially between parents and teachers. The Department seeks to establish a secure, appropriate virtual learning space that will be available, during and after regular school hours. In essence, Internet access hopefully can function as an all encompassing “home base” for the instructional business of the entire community of learners embraced by the public schools of New York City. Through Internet access, students, parents, and educators will have extended access to learning opportunities at home, at public libraries, or at any other location at which the Internet can be reached.

ACCEPTABLE USE POLICY

A. GENERAL PRINCIPLES OF ACCESS

1) The Department of Education of the City of New York (the “Department") is obtaining access to the Internet, including access to e-mail, for its employees, Department members, students, and guests. Guests include but are not limited to parents, substitute teachers, temporary Department employees, parent volunteers, and other school volunteers.

2) Internet access and the use of e-mail through the use of the Department's system, has a limited educational purpose. The term "educational purpose" includes use of the system by students and their parents for learning activities both in school and at home, employee professional or career development, communication between teachers, students and their parents and the facilitation of information-sharing between teachers and administrators throughout the New York City school system. If any user has a question whether their Internet use is consistent with the Department’s educational purpose, goals, and mission, s/he should consult with the appropriate supervisor, principal, teacher, etc.

This Internet Acceptable Use Policy governs all electronic activity, including e-mail and access to the Internet, which is undertaken by Department of Education employees, students, and parents/guardians either in their official Department of Education capacity or as part of the educational, instructional or extracurricular programs connected to the Department. No Department of Education employee, student, or parent/guardian may engage in activities prohibited by this IAUP, whether through the Department's Internet service or through another Internet Service Provider, when those activities are undertaken either in their official Department of Education capacity or as part of the educational, instructional, or extracurricular programs of the Department of Education.

As with other curricular offerings and tools, parents do not have a general right to opt their child out of classroom use of the Internet. As set forth more fully below however, parental consent is required with respect to certain aspects of Internet use (e.g., posting a child's photograph on a school web page). Parents moreover, are strongly encouraged to discuss and monitor their child's school Internet use and to discuss any issues or concerns that they may have with the school's teacher and administrators.

3) Student access to the Internet will be governed by this policy, related Department regulations, and the Citywide Standards of Conduct and Uniform Disciplinary Measures ("the student disciplinary code"). Employee use will be governed by this policy, related Department regulations, Department employment policy, and applicable collective bargaining agreements. All use will be in compliance with the acceptable use provisions of the Internet service provider.

4) The Department reserves the right to terminate any user's access to the Internet, including access to e-mail, at any time and for any reason. The Department reserves the right to monitor all Internet access, including all e-mail, through use of the Department's system. The Department specifically reserves the right to revoke access and/or take other appropriate disciplinary action, with respect to any user who violates this policy.

B. SYSTEM RESPONSIBILITIES

1) The Chancellor, or his/her designee, will serve as the coordinator to oversee Internet access via use of Department systems.

2) District staff are responsible for the dissemination of this Internet

Acceptable Use Policy and will work with schools to enforce this policy.

3) Each district must adopt a written district plan for the implementation of this policy by September 2001. Each district's plan must designate, for each school building in the district, a building-level coordinator for the Department's Internet and e-mail system and must include a customer service telephone number for users to call with questions or comments about the Internet Acceptable Use Policy. The building-level coordinator may be the building principal or his/her designee. The building-level coordinator will approve building-level activities, ensure teachers receive proper training in the use of the system and of this policy, establish a system to ensure adequate supervision of students using the system, maintain executed user agreements if applicable and be responsible for interpreting the Internet Acceptable Use Policy at the building level. Although this Internet Acceptable Use Policy does not require execution of user agreements by students or employees, the District may institute such a district-wide or school-based requirement. All district plans must also establish a process for modifying the Internet filtering software or for defiltering.

4) The Department reserves the right to revise this Internet Acceptable Use Policy as it deems necessary and will post the current policy on its web site as notice to users of any revisions. Users are responsible for reading the policy regularly.

5) Users who require technical assistance with Internet access or e-mail should call the Department of

Education Help Desk at (718) 935-5100.

C. LIMITATION OF LIABILITY

1) The Department makes no warranties of any kind, either express or implied, that the functions or the services provided by or through the Department system will be error-free or without defect. The Department will not be responsible for any damage users may suffer, including but not limited to, loss of data or interruptions of service. The Department is not responsible for the accuracy or quality of the information obtained through or stored on the system. The Department will not be responsible for financial obligations arising from a user's unauthorized use of the system.

2) Users will indemnify and hold the Department and its respective districts harmless from any losses sustained by the Department as a result of intentional misuse of the system by user.

D. FILTERING

The Department has installed Internet filtering software in an attempt to block user access to inappropriate and/or harmful text on the Internet. The software works by scanning web site addresses, web site content, e-mail and other documents for objectionable words or concepts. Objectionable words and concepts are pre-determined by the Department. When the software finds any such objectionable words or concepts, it denies the user access to them based on the level of access assigned to the word or concept by the Department. Generally, levels of access go from the least restrictive level, which allows users access to the web site or document that contains the word or concept, to the most restrictive level, which denies users access to the web site or document that contains the word or concept. There are levels between these two levels that neither automatically allow or automatically deny access but rather, prompts the software to perform a more in-depth review of the web site or document to determine whether it is objectionable (e.g., for high school students, the word or concept "breast" would fall into this intermediate level so a student who is doing research on breast cancer would be allowed access to web sites or documents related to "breasts" but a student looking for pornography would be denied access to pornography related to "breasts"). Filtering technology is not perfect and therefore, may in effect interfere with legitimate educational research.

The default level of access that will be granted to students varies depending on grade level and are referenced in subsections a, b, and c below. Each district shall establish a process for modifying the filter or for defiltering Internet access for students when it is educationally appropriate. The district process must indicate whether defiltering requests are to be approved at the district or school level and appropriate monitoring mechanisms must be established by the district. No filtering software is one hundred percent effective and it is possible that the software could fail. In the event that the filtering software is unsuccessful and children gain access to inappropriate and/or harmful material, the Department will not be liable.

a) Default filtering levels for grades Kindergarten through 5: The filter is set at the most restrictive setting in restricting access to Internet sites that may contain interactive chat or mail or information regarding:

- crime
- intolerance
- violence
- sex acts
- sex attire
- sex/nudity
- sex/personal
- basic sex education
- advanced sex education
- sexuality
- sports

b) Default filtering levels for grades 6 through 8:
Same setting as Kindergarten through 5 above.

c) Default filtering levels for grades 9 through 12:
The filter is modified to be less restrictive consistent with age and educational goals.

E. REGULATIONS OF ACCESS

1) Review of Access Privileges

a) The Department will cooperate fully with local, state, or federal officials in any lawful investigation concerning or relating to any illegal activities conducted through the Department system.

b) The Department may revoke Internet access in its sole discretion. If a student's access is revoked, the Department will ensure that the student nonetheless continues to have a meaningful opportunity to participate in the educational program.

c) Student disciplinary actions should be tailored to meet specific concerns related to the violation and to assist the student in gaining the self-discipline necessary to behave appropriately on an electronic network. If the alleged violation also involves a violation of other provisions of the student disciplinary code, the violation will be handled in accordance with the applicable provision of the code.

d) Employee violations of the Department Internet Acceptable Use Policy will be handled by appropriate discipline.

2) Privacy

a) The Department reserves the right to use "cookies" on its site. Cookies are computer programs that allow the Department, among other things, to verify whether a visitor is an authorized user of the Department's system and that store information about a user on a computer hard drive or disk. Information stored includes, but may not be limited to, the date and time a user visits the site and information about the user’s activities while online. Any information gathered is obtained solely for the purpose of improving the Department’s services and providing the system with statistical information to assist in improving teaching and learning by teachers and students respectively.

Except as otherwise provided in this Internet Acceptable Use Policy, the Department will not use cookies to gather personal identifying information about any of its users. Personal identifying information includes, but is not limited to, names, home addresses, e-mail addresses and telephone numbers.

b) As required by the Children’s Internet Protection Act (“CIPA”), the Department will monitor students’ online activities. Such monitoring may lead to discovery that the user has violated or may be violating, the Department Internet Acceptable Use Policy, the student disciplinary code, or the law. The Department also reserves the right to monitor other users (e.g., non students) online activities.

c) The Department reserves the right to employ and review the results of software that searches, monitors and/or identifies potential violations of the Internet Acceptable Use Policy.

d) Users should be aware that their personal files may be discoverable in court and administrative proceedings and in accordance with public records laws.

e) System users have no privacy expectation in the contents of their personal files and records of their online activity while on the Department system.

3) Freedom of Expression

Department policies on Freedom of Expression, as set forth in the Bill of Student Rights and Responsibilities will govern the use of the Internet. Nothing in this policy shall affect any existing or future policy on free speech.

4) Selection of Material

When using the Internet for class activities, teachers should:

a) Select material that is appropriate in light of the age of the students and that is relevant to the course objectives.

b) Preview the materials and sites they require students to access to determine the appropriateness of the material contained on or accessed through the site.

c) Provide guidelines and lists of resources to assist their students in channeling their research activities effectively and properly.

d) Assist their students in developing the skills to ascertain the truthfulness of information, distinguish fact from opinion, and engage in discussions about controversial issues while demonstrating tolerance and respect for those who hold divergent views.

5) Parental Notification and Responsibility

a) As appropriate, the Department will provide students and parents with guidelines and instructions for student safety while using the Internet.

b) The Department Internet Acceptable Use Policy contains restrictions on accessing inappropriate material and student use generally will be supervised. However, there is a wide range of material available on the Internet, some of which may or may not fit the particular values of the students. It is not practically possible for the Department to monitor and enforce a wide range of social values in student use of the Internet. Further, the Department recognizes that parents bear primary responsibility for transmitting their particular set of family values to their children. The Department will encourage parents to specify to their child(ren) what material is and is not acceptable for their child(ren) to access through the Department system.

c) If the Department provides home Internet access, parents are exclusively responsible for monitoring their own and their child(ren)'s use of the Internet if they access the system from home. Filtering may or may not be employed to screen home access to the Internet. Parents should inquire with the school or district.

6) Access

a) Students: Students may be provided with Internet access and may have dial-up access to the system from home. There is no central Department policy requiring a district or school to enter into a written agreement to provide a student such access. On the other hand, for educational reasons, a district may decide to create a written agreement or “compact” with parents that embodies the terms and responsibilities of the student, parent and school in detail. However, the written agreement may not permit any Internet or e-mail activity prohibited by this Internet Acceptable Use Policy, and it may not prohibit any such activity permitted by this Policy.

b) Department Employees: Department employees may be provided with Internet accounts and may have dial-up access to the system. No written agreement will be required.

7) Limitations on Internet Usage

A) Personal Safety Violations For Students

i) Student users will not post or transmit photographs or personal contact information about themselves or other people without prior written parental consent from the parent of the student whose information is being posted. Such consent must be delivered to the child’s teacher or principal. Personal contact information includes, but is not limited to, home address, telephone number, school name, school address and classroom.

ii) Student users will not agree to meet with someone they have met online without their parent's approval and participation.

iii) Student users will promptly disclose to their teacher or other school employee any message they receive that is inappropriate or makes them feel uncomfortable.

B) Illegal Activities

i) Users shall not attempt to gain unauthorized access to the Department system or to any other computer system through the Department system, or go beyond their authorized access. This prohibition includes intentionally seeking information about passwords belonging to other users, modifying passwords belonging to other users, or attempting to log in through another person's account. Further, users may not attempt to access, copy, or modify another user's files. These actions are not permitted and may be illegal, even if only for the purposes of "browsing."

ii) Users shall not attempt to subvert network security, impair the functionality of the network or bypass restrictions set by network administrators. Users are also prohibited from destroying data by spreading computer viruses or vandalizing data, software or equipment.

iii) Users shall not use the Department system to engage in any other illegal act, such as arranging for a drug sale, purchasing alcohol for a minor, engaging in criminal gang activity, threatening the safety of a person, etc.

C) System Security Violations

i) Users are responsible for the use of their individual account if applicable and should take all reasonable precautions to prevent others from being able to use their account. Under no conditions should a user provide their password to another person, except that supervisors and/or teachers may require users to provide their passwords.

ii) Student users will immediately notify a teacher if they identify a possible security problem (such as disclosure of their password to another person) and other users will immediately notify the system administrator. No users will go looking for security problems, because this may be construed as an illegal attempt to gain access.

iii) Every school must install and maintain anti-virus software on each workstation. Updates, typically referred to as "virus definitions," should be updated as the manufacturer recommends.

D) Inappropriate Language

i) Restrictions against inappropriate language apply to public messages, private messages, and material posted on Web pages.

ii) Users will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, abusive or disrespectful language.

iii) Users will not post information that could interfere with the educational process or cause a danger of disruption in the educational environment.

iv) Users will not engage in personal attacks, including prejudicial or discriminatory attacks.

v) Users will not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a user is told by a person to stop sending them messages, they must stop. However, nothing in this paragraph shall prohibit supervisory use of e-mail in connection with Department activities and employment.

vi) Users will not knowingly or recklessly post false or defamatory information about a person or organization.

E) Privacy Violations

i) Users should not repost a message that was sent to them privately without permission of the person who sent them the message.

ii) Users should not post private information about another person.

F) Respecting Resource Limits

i) Users will use the system only for educational and professional activities.   Staff may not use the Internet for personal use during working hours, except that they may engage in incidental use during their duty-free time (e.g., staff may be permitted to use the Internet for purchasing a book for personal use during their lunch hour, but may not operate a business or engage in any profit-making activity at any time).

ii) Users will not download large files unless absolutely necessary. If necessary, users will download the file at a time when the system is not being heavily used and immediately remove the file from the system computer to their personal computer or diskette.

iii) Users will not post chain letters or engage in "spamming." Spamming is sending an annoying or unsolicited message to many people, except that an unsolicited message sent by a supervisor, relating to work activity does not constitute spamming.

iv) Users will check their e-mail frequently and delete unwanted messages promptly. Users will limit the size of their mailboxes to a district-identified storage limit. The system will notify users when they are approaching the limit and users will not be able to send e-mail once they have exceeded a defined limit, currently 30 megabytes. However, users may still be able to receive and view e-mail upon exceeding the limit.

v) Users will not send e-mail containing commercial links unless the link is predominantly instructional in nature (as described in Section 8, B, ii, d of this policy).

G) Plagiarism and Copyright Infringement

i) Users will not plagiarize works that they find on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were original to the user.

ii) Users will respect the rights of copyright owners and not infringe on those rights. Copyright infringement occurs when an individual inappropriately reproduces a work that is protected by a copyright. If a work contains language that specifies acceptable use of that work, the user should follow the expressed requirements. If the user is unsure whether or not they can use a work, they should request permission from the copyright owner.

H) Access to Inappropriate Material

i) Users will not use the Department system to access material that is profane or obscene (e.g., pornography), that advocates illegal or dangerous acts, or that advocates violence or discrimination towards other people (e.g., hate literature). For students, a special exception may be made if the purpose is to conduct research and is approved in writing by both the teacher and the parent. Department employees may access the above material only in the context of legitimate research expressly approved in writing by the employee's supervisor.

ii) If users inadvertently access such information, they should immediately disclose the inadvertent access in a manner specified by their school or central division office. This will protect users against an allegation that they have intentionally violated the Internet Acceptable Use Policy.

I) Other

i) Users will not use the Internet for advertising, promotion, commercial purposes or similar objectives, except that employees may make personal purchases online during their duty-free (e.g., lunch) time.

ii) Users will not use the Internet to conduct for-profit business activities or to engage in religious activities. Users are also prohibited from engaging in any non-governmental-related fund raising or public relations activities such as solicitation for religious purposes, lobbying for political purposes, or soliciting votes. The Department is not responsible for this or any other commercial activity users engage in.

8) Web Pages: The Department's Web page policy is as follows:

A) Student Information

Each school must obtain written parental consent prior to the disclosure of student information or student work on any Department Web page. Student information includes name, address, school name, grade, class, photograph, writing or other creative work, or any other student educational record.

B) Web Page Requirements

i) The provisions of this Internet Acceptable Use Policy will govern material placed on the Web.

ii) Web Pages shall not:

a) Contain personal contact information about students beyond that permitted by the school, district and parent.

b) Display photographs, videos or other images of any identifiable individual, other than a historical or public figure, without a signed release. Releases for students under the age of 18 must be signed by their parent or lawful guardian.

c) Contain copyrighted or trademarked material belonging to others unless written permission to display such material has been obtained from the owner. There will be no assumption that the publication of copyrighted material on a web site is within the fair use exemption.

d) Contain web links to or advertisements for profit-making entities, such as publishers or other consumer goods purveyors, unless the site being linked to is predominantly instructional in nature (such as museum sites, encyclopedias, national parks, aquariums, literary organizations, etc.). Notwithstanding the forgoing, districts and schools may not directly benefit financially from any such entities linked to on their web pages.

e) Display for promotional purposes, the logo or other commercial insignia of the vendor that created the web page.

iii) Material placed on the web site is expected to meet academic standards of proper spelling, grammar and accuracy of information.

iv) A student may have a copyright interest in material he or she has created and places on a web page covered by this Policy. Placing the material on the web page will not transfer the copyright interest to the Department. But students and parents should be aware that placing material on a web page may affect a copyright interest by giving other users access to the material. A Department employee will not have a copyright interest in material he or she has created and places on a web page covered by this Policy.

v) All web pages should include a notice that the web page may contain copyrighted material and that visitors may not download any such material without the prior consent and approval of the copyright owner.

vi) All Web pages should have a link at the bottom of the page that will help users find their way to the appropriate home page.

vii) Users should retain a back-up copy of their Web pages.

viii) Each district and each school may host one (1) web site on official New York City Department of Education web servers, but this is not a requirement. However, all district, school, teacher, staff, student, extracurricular organization and central office web sites not hosted by the Department may do so only if they register with the Department's Division of Instructional and Information Technology (DIIT). This ensures that in the event of hacking or any other violations of this policy that come to the Department's attention, DIIT can contact the appropriate parties. This requirement will also make it possible for Office of Legal Services to review the contracts between the district/school and the third party vendors that provide the hosting service to ensure that such contracts comply with the terms set forth in this policy.

C) District and Superintendent (“District(s)”) Web Pages

i) Material appropriate for placement on the District web pages includes: District information, school information, teacher or class information, student projects, and student extracurricular organization information. Personal, non-educationally-related information should not be allowed on District web pages.

ii) District Superintendents will designate a District Web Publisher, responsible for maintaining the official District web page and monitoring all District web activity. The Web Publisher will develop style and content guidelines for official District and school web page materials in accordance with the Division of Instructional and Information Technology (DIIT)/Office of Web Services (OWS) Policy, Procedures and Guidelines. The Web Publisher will also develop procedures for the placement and removal of such material. All official District and school material originating from the District posted on the District or a school Web page must be approved through a process established by the District Web Publisher. The District’s procedures may require approval of school web page material at either the district or school level.

D) School Web Pages

The building principal will designate a School Web Publisher, responsible for managing the school Web page and monitoring class, teacher, student, and extracurricular web pages subject to district procedures. All official material originating from the school must be consistent with the style and content guidelines developed by the School Web Publisher and approved through a process established by the School Web Publisher. The school Web Publisher will develop additional guidelines for the school Web page in accordance with DIIT/OWS Policy, Procedures and Guidelines.

E) Teacher Web Pages

Subject to district-wide policies and procedures, teachers may establish Web pages for use with class activities or to provide a resource for other teachers. Teachers will be responsible for maintaining their class or educational resource sites. Teacher web pages will not be considered official material, but will be developed in such a manner as to reflect well upon the Department, district and school.

F) Other Staff Web Pages

Subject to district-wide policies and procedures, staff may develop web pages that provide a resource for others. Staff will be responsible for maintaining their resource sites. Staff web pages will not be considered official material, but will be developed in a manner as to reflect well upon the Department, district and school.

G) Student Web Pages

i) Subject to district-wide policies and procedures, students may create a web site as part of a class activity. Material presented on a student class activity web site must meet the educational objectives of the class activity.

ii) Subject to District procedures and with the approval of the building principal or Web Publisher, students may establish personal web pages. Material presented in the student's personal web page must be related to the student's educational and career preparation activities.

iii) The District has the right to exercise control over the content and/or style of student web pages so long as its actions are reasonably related to legitimate pedagogical concerns. Requiring removal of material that fails to meet established educational objectives or that is in violation of a provision of the Internet Acceptable Use Policy or student disciplinary code will not be considered a violation of a student's right to free speech under the Student Bill of Rights. However, student material may not be removed on the basis of disagreement with the views expressed by the student.

iv) Student Web pages must include the following notice: “This is a student Web page. Opinions expressed on this page shall not be attributed to the New York City Department of Education or the student's school.”

v) Schools have the right to remove student web pages at the end of each school year.

H) Extracurricular Organization Web Pages

i) With the approval of the building principal, extracurricular organizations may establish web pages. Material presented on the organization web page must relate specifically to organization activities. The Department has the right to exercise control over the content and/or style of organization web pages so long as its actions are reasonably related to legitimate pedagogical concerns.

ii) Extracurricular organization web pages must include the following notice: "This is a student extracurricular organization web page. Opinions expressed on this page shall not be attributed to the New York City Department of Education.”

I) Central Office Web Pages

i) Central offices may establish web pages but material posted on the central office web page must relate specifically to the office’s services. The style and content of any central office web page must be consistent with the Department’s Division of Instructional and Information Technology (“DIIT”)/Office of Internet Management Services (“IMS”) Policy, Procedures and Guidelines.

9) E-mail Policy:

A) Email Acceptable Use Guidelines

i) “Acceptable” e-mail activities are those that conform to the purpose, goals, and mission of the DOE and to each user's job duties and responsibilities . Users shall have no right to privacy while using the DOE's internet or e-mail system . E-mail may not be used for personal purposes during working hours, except that users may engage in minimal e-mail activities for personal purposes, such as family correspondence, if the use does not diminish the employee's productivity, work product, or ability to perform services for the DOE.

“Unacceptable” use is defined generally as activities using DOE hardware, software, or networks at any time that does not conform to the purpose, goals, and mission of the DOE and to each user's job duties and responsibilities. The following list, although not inclusive, provides some examples of unacceptable uses:

1. Opening unknown e-mail attachments or introducing computer worms or viruses. Users are prohibited from performing any activity that will or may cause the loss or corruption of data or the abnormal use of computing resources (degradation of system/network performance).

2. Using e-mail services for private commercial or business transactions and any activity meant to foster personal gain.

3. Using your DOE e-mail address to subscribe to websites or other internet services that do not conform to your DOE duties and responsibilities.

4. Conducting non-Department of Education fund raising or public relations activities such as solicitation for religious and political causes or not-for-profit activities.

5. Transmitting threatening, offensive harassing information (messages or images) containing defamatory, abusive, obscene, pornographic, sexually oriented, racially offensive, or otherwise biased, discriminatory, or illegal material.

6. Attempting to subvert network security, impair functionality of the network, or bypass restrictions set by the network administrators. Assisting others in violating these rules by sharing information or passwords.

7. Distributing "junk" mail, such as chain letters, advertisements, or unauthorized solicitations.

8. Revealing, publicizing, using, or reproducing confidential or proprietary information regarding the DOE including, but not limited to, financial information, databases and/or the information contained therein, computer network access codes, staff or student information and business relationships.

Users should contact their supervisors about questionable e-mail usage.

This e-mail Acceptable Use (EAU) applies to all Department of Education (DOE) employees, temporary employees, consultants, contractors, and anyone given access to e-mail via any DOE electronic device, network, or e-mail service owned, provided or maintained by the DOE . The acceptable uses are an integral part of the DOE Internet Acceptable Use Policy.

Users should call the Help Desk at (718) 935-5100 if they experience any problems with opening documents; believe they may have a computer virus, or encounter questionable material or potential threats to the DOE's internet or e-mail system.

NOTE: Users may be subject to limitations on their use of e-mail as determined by their supervisor. The DOE reserves the right to examine any/all e-mail or Internet correspondence for security and/or network management purposes.

Violation of this e-mail policy may result in disciplinary action.