Department of Education

Internet Acceptable Use and Safety Policy
Implementing Department Resolution of February 14, 2001
Revised as of July 1, 2012

INTERNET ACCEPTABLE USE AND SAFETY POLICY (IAUSP)

The Policy

The NYC Department of Education ("**Department**") provides access to the Department's Internet Systems for its employees, agents, students, and volunteers, collectively referred to as "**users**" for educational and business purposes, in conformance with applicable law. This Internet Acceptable Use and Safety Policy ("**policy**") governs all electronic activity of users using and accessing the Department's Internet systems, including Department e-mail and Department-provided access to the Internet, and applies to the use of the Department Internet Systems both on and off Department property.

"**The Department's Internet Systems**" means Department-provided devices, Internet connections (including wireless connections) provided by the Department, Department-provided e-mail accounts, intranet and any remote connection to Department systems. A user is deemed to access and use the Department's Internet Systems through any electronic activity conducted on the Department's Internet Systems using any device (whether or not such device is a Department-provided device) regardless of the user's physical location.

"**Department-provided devices**" means any electronic device provided by the Department, including, but not limited to, desktop computers, laptops, and hand-held devices, such as personal digital assistants (PDAs), smartphones, iPads, tablets and e-readers.

Student use of the Department's Internet Systems is governed by this policy, Department regulations, policies and guidelines, the Citywide Standards of Conduct and Uniform Disciplinary Measures (the "**Discipline Code**") and applicable law. Employee use is governed by this policy, Department regulations, policies and guidelines, the Department's employment policies, applicable collective bargaining agreements and applicable law.

By using the Department's Internet Systems, a user agrees to follow this policy and all applicable Department regulations, policies and guidelines. All users must report any misuse of the network or Internet or receipt of any communication that violates this policy to a teacher, supervisor or other appropriate Department personnel.

Principles of Acceptable and Safe Internet Use

General

Internet access and e-mail provided by the Department are intended for educational use, instruction, research and the facilitation of communication, collaboration, and other Department related purposes. Users are subject to the same standards expected in a classroom and/or professional workplace.

Monitoring and privacy

Users have no right to privacy while using the Department's Internet Systems. The Department monitors users' online activities and reserves the right to access, review, copy, store, or delete any electronic communications or files. This includes any items stored on Department-provided devices, such as files, e-mails, cookies, and Internet history.

The Department reserves the right to disclose any electronic activity, including electronic communications, to law enforcement officials or third parties, as appropriate and consistent with applicable law. The Department will fully

cooperate with local, state, or federal officials in any lawful investigation concerning or relating to any illegal activities conducted through the Department's Internet Systems.

Prohibited Uses of the Department's Internet Systems
Users may not engage in any of the activities prohibited by this policy when using or accessing the Department's Internet Systems.

If a user is uncertain whether behavior is prohibited, he or she should contact a teacher, supervisor or other appropriate Department personnel. The Department reserves the right to take immediate action regarding activities that (1) create security and/or safety issues for the Department, students, employees, schools, network or computer resources, or (2) expend Department resources on content the Department determines lacks legitimate educational or Department content or purpose, or (3) the Department determines are inappropriate.

Below is a non-exhaustive list of examples of prohibited behavior:

1. Causing harm to others, damage to their property or Department property, such as:

    a. Using, posting or distributing profane, lewd, vulgar, threatening, or abusive language in e-mail messages, material posted on Department web pages, or professional social media sites;
    b. Accessing, using, posting, or distributing information or materials that are pornographic or otherwise obscene, advocate illegal or dangerous acts, or advocate violence or discrimination. If users inadvertently access such information, they should immediately disclose the inadvertent access in a manner specified by their school or central division office;
    c. Accessing, posting or distributing harassing, discriminatory, inflammatory, or hateful material, or making damaging or false statements about others;
    d. Sending, posting, or otherwise distributing chain letters or engaging in spamming;
    e. Damaging computer equipment, files, data or the Department's Internet System in any way, including spreading computer viruses, vandalizing data, software or equipment, damaging or disabling others' electronic property, or engaging in conduct that could interfere or cause a danger of disruption to the Department's educational or business environment;
    f. Using the Department's Internet System in a manner that interferes with the education of the user or others or the job duties of the user or others;
    g. Downloading, posting, reproducing or distributing music, photographs, video or other works in violation of applicable copyright laws. Any music, photographs and/or video should only be downloaded for Department, and not personal purposes. If a work specifies how that work may be used, the user should follow the expressed requirements. If users are unsure whether or not they can use a work, they should request permission from the copyright or trademark owner; or
    h. Engaging in plagiarism. Plagiarism is taking the ideas or writings of others and presenting them as if they were original to the user.

2. Gaining or attempting to gain unauthorized access to the Department's Internet Systems, or to any third party's computer system, such as:

    a. Malicious tampering, phishing or hacking activities;
    b. Intentionally seeking information about passwords belonging to other users;
    c. Disclosing a user's password to the Department's Internet Systems to other individuals. However, students may share their Department password with their parents.
    d. Modifying passwords belonging to other users;
    e. Attempting to log in through another person's account;
    f. Attempting to gain access to material that is blocked or filtered by the Department;

g. Accessing, copying, or modifying another user's files without authorization;
h. Disguising a user's identity;
i. Using the password or identifier of an account that does not belong to the user; or
j. Engaging in uses that jeopardize access into others' accounts or other computer networks.

3. Using the Department's Internet Systems for commercial purposes, such as:

   a. Using the Department's Internet Systems for personal financial gain;
   b. Conducting for-profit business activities, personal advertising, or other non-Department business communications;
   c. Engaging in fundraising (except as set forth in the Chancellor's Regulation A-610); or
   d. Using the Department's Internet Systems on behalf of any elected official, candidate, candidates, slate of candidates or a political organization or committee.

4. Engaging in criminal or other unlawful activities.

Filtering

In accordance to Children's Internet Protection Act ("**CIPA"**), the Department blocks or filters content over the Internet that the Department considers inappropriate for minors. This includes pornography, obscene material, and other material that may be harmful to minors. The Department may also block or filter other content deemed to be inappropriate, lacking educational or work-related content or that pose a threat to the network. The Department may, in its discretion, disable such filtering for certain users for bona-fide research or other lawful educational or business purposes.

Users shall not use any website, application, or methods to bypass filtering of the network or perform any other unlawful activities.

For additional information regarding CIPA see link below:

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

Protection of Personally Identifiable & Confidential Information

The Family Educational Rights and Privacy Act ("**FERPA**") prohibits Department school officials from disclosing personally identifiable information ("**PII**") from education records of Department students and families to third parties without parental consent. However, several exceptions to this general rule may apply.

All users of the Department's Internet Systems must comply with FERPA and Chancellor's Regulation A-820, Confidentiality and Release of Student Records; Records Retention. If you are unsure about whether the activity will comply with FERPA or Chancellors Regulation A-820, please contact the Department's Chief Information Security Officer.

Internal communications with a Department attorney may also be confidential. Accordingly, users should not forward or distribute such communications without first checking with the attorney. Users should ensure that e-mails that include or attach confidential information are only sent to the intended recipients.

Student Internet Safety

1. Department Responsibilities:

Department of Education

a. The Department will provide curriculum about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response.

b. The Department will work to protect the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications.

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

2. Students Using the Department's Internet Systems

a. Students must not reveal personal information about themselves or other persons on social networking sites, in chat rooms, in emails or other direct electronic communications, or any other forum over the Internet. For example, students must not reveal their home address, or telephone or cell phone number. Students must not display photographs of themselves, or the images of others.

b. Students should not meet in person anyone they have met only on the Internet.

c. Students must promptly disclose to their teacher or other school employee any message or other activity they receive that is inappropriate or makes them feel uncomfortable.

d. Students should not allow Department computers to save their passwords.

3. Teachers using the Department Internet Systems, including Social Media for class activities

a. Teachers should educate students about appropriate and safe online behavior, including interacting with individuals on social networking websites and in chat rooms and cyberbullying awareness and response. Teachers should refer to the Department's Citizenship in the Digital Age guide, and other free educational Internet safety resources available on the Internet.

b. Social Media

- "**Social media**" means any form of online publication or presence that allows interactive communication, including, but not limited to, social networks, blogs, Internet websites, internet forums, and wikis. Examples of social media include, but are not limited to, Facebook, Twitter, YouTube, Google+, and Flickr.
- Schools use a variety of online web-based interactive communication technologies to enhance students' education and learning. Social media sites must be used only for educational and school related purposes, in connection with lessons and assignments and to facilitate communication with teachers and other students.
- The Department limits access to these sites to individuals within the Department and Department school officials. If access to a social media site will extend beyond individuals within the Department or Department school officials, then parent consent is required.
- Teachers must refer to the Department's Social Media Guidelines, which are incorporated into this policy, if Internet activities will involve social media.

4. Parents:

   a. Although students generally will be supervised when using the Department's Internet System on school property, it is not practicable for the Department to monitor and enforce a wide range of social values in student use of the Internet. Parents are primarily responsible for transmitting their particular set of family values to their children, and discussing with their children what material is and is not acceptable for their children to access through the Department's Internet Systems.

   b. Parents are exclusively responsible for monitoring their children's use of the Internet when the Department's Internet Systems are accessed from home or a non-school location. The Department may or may not employ its filtering systems to screen home access to the Department's Internet Systems. Parents should inquire with the school or Department.

Violations of this Policy
The Department, including central offices and schools, reserves the right to terminate any user's access to Department Internet Systems - including access to Department e-mail - at any time.

If a student violates this policy, appropriate disciplinary action will be taken consistent with the Discipline Code and applicable Chancellor's Regulations. If a student's access to the Department's Internet System is revoked, the student may not be penalized academically, and the Department will ensure that the student continues to have a meaningful opportunity to participate in the educational program.

Employee violations of this policy will be handled by appropriate discipline.

All users must promptly disclose to their teacher, supervisor, principal or manager any information they receive that is inappropriate or makes them feel uncomfortable.

Limitation of Liability
The Department makes no guarantees about the quality of the services provided and is not responsible for any claims, losses, damages, costs, or other obligations arising from use of the network or accounts. Any additional charges a user accrues due to the use of the Department's network are to be borne by the user. The Department also denies any responsibility for the accuracy or quality of the information obtained through user access. Any statement, accessible on the computer network or the Internet, is understood to be the author's individual point of view and not that of the Department, its affiliates, or employees.

Copies of this Policy and Inquiries
The Department reserves the right to amend and/or revise this policy at any time as the need arises. This policy is available upon request and on the Department's website located at http://schools.nyc.gov/Offices/EnterpriseOperations/DIIT/WebServices/iaup/default.htm#preamble.

Inquiries pertaining to this regulation should be addressed to:

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