6415 C
Internet, E-mail and Network Rules for Staff Use

Regulation 6415 C

Original Adoption: 05/26/2009
Revision Dates: 08/12/2014
Review Date: 4/17/2012

Effective Date: 08/13/2014

I. PURPOSE

The purpose of this regulation is to establish appropriate rules for educational and ethical staff uses of the Internet, e-mail and District networks at work and to identify individual staff responsibilities.

II. GENERAL STATEMENTS REGARDING DISTRICT COMPUTER SYSTEMS

A. Computer resources are assets of the Minneapolis Public Schools and are to be protected from unauthorized access, modification, destruction or disclosure.

B. All acquisitions whether by purchase or otherwise of hardware or software must be approved in advance by the Information Technology Department to assure conformation with the District hardware and software systems.

C. All staff seeking remote access to the District Network shall submit an application to the District Information Technology Department in a form determined by that department. Determinations of access shall be the joint responsibility of the requestor's supervisor and the District Information Technology Department. Remote Access users must follow recommended security practices of the network including the use of updated antivirus software.

D. Minneapolis Public Schools reserves the right to monitor computer systems and to read and copy all files or data contained on any District computer (including, but not limited to, e-mail messages) at any time and without prior notice.

E. Staff shall not vandalize, damage or disable the technology, property or systems used by the Minneapolis Public Schools, another person or organization.

F. Staff shall not make deliberate attempts to degrade or disrupt equipment, software, or system performance by spreading computer viruses or performing other disruptive acts.

G. Staff shall not tamper with, modify or change the District system software, hardware or wiring or take any action to violate the District's computer security system.

H. Only personnel authorized by the District's technology department may
   1. load software onto any Minneapolis Public Schools computer,
   2. connect any hardware or other equipment to any Minneapolis Public Schools computer or

3. move or change any Minneapolis Public Schools computer equipment.

I. Staff authorized to connect peripheral technologies such as projectors, document cameras and printers shall comply with fire marshal and Occupational Safety and Health Administration (OSHA) regulations as directed by District technology personnel.

J. Guests or staff with non-District computers are required to have a building technology assistant or District technology staff check their computers to ensure that the computer has an updated operating system software and updated virus detection and isolation software before connecting the computer to the District network to ensure network integrity and security.

III. USE OF PERSONAL DEVICES

A. Staff may use personally owned electronic devices to access the District's internet access, wireless services and District provided e-mail system.

B. Staff who use internet capable devices owned by persons other than the District to access the Internet or District provided email addresses or web sites while using District internet access are subject to the same rules and policies as if they were using a district provided device.

C. Personally owned computers may not be physically connected to the District network. They may be used as stand-alone devices, and may be used wirelessly to connect to the internet through District access. Nothing in this section prohibits the use of personally owned computers or devices that are electronically connected to the District network through a duly authorized VPN (virtual private network) connection.

D. The District is not responsible neither for assuring that the personally owned device is appropriately connected to the internet, nor that any of its hardware or software remains in working condition nor is or remains configured for internet use.

E. Personally owned devices are brought to work and used by staff at their own risk; the District accepts no responsibility for loss or damage to personally owned devices brought to work by staff. Internet access through personally owned devices shall have the same filtered access to the internet as district owned devices while accessing the internet through District wireless services. However no filtering is provided if access is obtained through other wireless providers.

F. Portable external data storage and drives, such as flash drives, jump drives, or thumb drives and the like may be connected to district computers for the purposes of transferring, backing up or transporting personal files from a student or staff account. Use of such devices to transfer, copy or install unlicensed or malicious software is

prohibited, and any use therefore shall subject the user to discipline, including paying the costs of repair or recovery to any files or computer hardware or software affected.

G. Inappropriately connected or used personal devices must be disconnected immediately at the request of the supervisor or any Information Technology staff member. Failure to do so will result in the confiscation of the personal device. Confiscated devices shall be returned to the staff at the end of the employee's school or work day. Other disciplinary actions may also be taken based on the use of the device and under other district policies.

H. Personal devices may be searched by district personnel upon reasonable suspicion that the device has been used inappropriately under district policies and rules.

IV. ELECTRONIC MAIL (E-MAIL)

A. The primary purpose of electronic mail (e-mail) provided through District systems is business communications of Minneapolis Public Schools and its customers.

B. The e-mail system should not be used to solicit for or promote any outside business ventures or for any political or religious purposes unless specifically authorized by Minneapolis Public Schools.

C. All e-mail received through or generated by District computers are District property, regardless of subject matter and are subject to review by District authorities at any time. The existence of passwords or "message delete" functions does not restrict or eliminate District authority to access electronic communications.

D. Appropriate language and standards of decency must be used in communicating through District e-mail accounts. Offensive, demeaning, defamatory, harassing or disruptive messages are prohibited.

E. Staff must maintain private, confidential or proprietary information in an e-mail as required by the Minnesota Data Practices Act and district policy.

F. Staff shall not provide district e-mail account access to an unauthorized person or access another user's district e-mail without authorization.

G. Staff may subscribe to an Internet mailing list only if the subscription is:
   1. work related, or
   2. does not generate numerous messages.

H. Employees are expected to use their district assigned email account for all district business. Alternate email accounts, including free Gmail or Yahoo accounts, etc, should be used for personal purposes.

V. INTERNET ACCESS

A. District connection to the Internet is primarily for work-related purposes.

B. The District shall use a filter to limit the Internet environment available through the District system to provide access to the most appropriate sites and materials for staff and students.

C. Inappropriate uses of District Internet Access include, but are not limited to:
   1. posting, viewing, downloading or otherwise receiving or transmitting offensive, defamatory, pornographic or sexually explicit material;
   2. posting, viewing, downloading or otherwise receiving or transmitting materials that use language or images that advocate violence or illegal discrimination toward other people (hate literature);
   3. posting, viewing, downloading or otherwise receiving or transmitting material that may constitute harassment or discrimination contrary to District policies regarding discrimination, harassment or violence;
   4. engaging in computer "hacking" or other related activities;
   5. attempting to or actually disabling or compromising the security of information on any computer, regardless of location;
   6. engaging in any illegal act in violation of any local, state or federal ordinance, statute or law.

D. Staff may participate in public Internet discussion groups using District access, but only to the extent that such participation is:
   1. work related
   2. does not reflect adversely on Minneapolis Public Schools,
   3. is consistent with all Minneapolis Public Schools standards and policies (including those regarding confidential information and public statements), and
   4. does not express any position that is, or may be reasonably interpreted as, inconsistent with any position taken by Minneapolis Public Schools.

E. Other than as allowed herein, any other posting using Minneapolis Public Schools name or otherwise identifying Minneapolis Public Schools must be approved in advance by the Communications Department.

F. Staff shall not:
   1. use proxy servers to access Internet content that is blocked by Minneapolis Public Schools filters.
   2. use district access to post unauthorized or inappropriate personal information about a user or another individual on a social network site.

G. Staff will observe all copyright laws. Information posted, viewed or downloaded from the Internet may be protected by copyright. Staff shall reproduce copyrighted material or information from the Internet only if such reproduction is:

1. a fair use, or
2. based on express permission given by the copyright owner.

H. All files downloaded from the Internet must be checked for possible computer viruses. The District authorized virus checking software installed on each District computer will ordinarily perform this check automatically, however a user should contact authorized district personnel before downloading any file if the user has a question about a potential virus or has reason to believe that the file poses particular risks.

VI. RESPONSIBILITIES

A. Staff that are transferring from or leaving a position shall leave all work-related files, electronic or physical, including form letters, handbooks, databases, procedures and manuals, regardless of authorship, for their replacement, or in the possession of their supervisor.

B. Individual passwords for computers are confidential and may not be shared or posted.
   1. If a user's password is learned by another, it should be changed immediately.
   2. Each user is responsible for any activity performed using the person's password.
   3. No user should attempt to gain access to another's documents without prior authorization.
   4. An active terminal with access to student data shall not be left unattended, and shall be further protected by password protected screen savers.
   5. A generic login, one which does not give access to student or personnel data, may be used when a computer will be accessible by persons other than the primary user.

C. Staff are expected to know how to use the technology necessary to perform the duties of their position.
   1. Staff should participate in technology training as identified as useful for the performance of their duties.
   2. From time to time the District may require training for specific technology uses.

D. Staff shall acknowledge that they have received and read the Internet and Educational Network Use Policy and Regulations in a format determined by the District.

E. Failure to comply with this regulation shall subject the person to discipline according to the terms of their collective bargaining agreement, or contract, which discipline may include suspension or withdrawal of internet or e-mail access, payment for damages or repair, termination, and referral to civil or criminal authorities for prosecution.

Legal References:
15 USC §6501 *et seq.* (Children's Online Privacy Protection Act)

17 USC §101 *et seq.* (Copyrights)
20 USC §6751 *et seq.* (Enhancing Education through Technology Act of 2001)
47 USC §254 (Children's Internet Protection Act of 2000 [CIPA])
47 CFR §54.520 (FCC Rules implementing CIPA)
Minn. Stat. §125B.15 (Internet Access for Students)
Minn. Stat. §125B.26 (Telecommunications/Internet Access Equity Act)
Tinker v. Des Moines Indep. Cmty. Sch. Dist., 393 U.S. 503, 89 S.Ct. 733, 21 L.Ed.2d 731 (1969)
United States v. American Library Association, 539 U.S.194, 123 S.Ct.2297, 56 L.Ed.2d 221 (2003)
Layshock v. Hermitage Sch. Dist., 412 F.Supp.2d 502 (2006)
J.S. v. Bethlehem Area Sch. Dist., 807 A.2d 847 (Pa. 2002)

Cross References:
MPS Policy 1040 (Student and Staff Data Protection)
MPS Policy 4002 (Harassment and Violence Prohibition)
MPS Policy 5000 (Equal Education Opportunity)
MPS Policy 5200 (Behavior Standards)
MPS Policy 5201 (Bullying and Hazing Prohibition)
MPS Policy 6415 (Internet and Educational Network Use)