

SUBJECT: **INTERNET USAGE**

Supersedes: DPS Policy 10.09 - Internet and Use Of The DPSnet, July 14, 2000

Effective: February 15, 2005

Pages: 1 of 5

1.0 POLICY PURPOSE

Detroit Public Schools' (DPS) Internet and Intranet environment is available to assist business processes through the utilization of technology and technology related services. Among the essential components of internet usage management are: establishing guidelines for utilization, a means for securing sensitive data and applications; awareness of the monitoring and recording Internet usage; assist in the training of end-users in the proper use of all available access and security technology, search engines usage, and encryption tools.

Appropriate Internet usage is important for three central reasons:

1. **Employee Productivity:** Organizations typically measure productivity based on specified goals and objectives, as well as by examining how employees allocate their time. Management should have the information it needs to examine how employees spend their time on the Internet.
2. **Network Bandwidth and Resources:** Internet access is not free. Excessive non-business usage of the Internet results in real costs to the organization. For example: the cost to upgrade network resources such as leased lines, routers, disk storage, and printers in order to handle increased load; as well as the cost of wasted time caused by slow network response or unreliable connections;
3. **Potential Legal Liabilities and/or Negative Publicity:** Inappropriate usage of the Internet may result in legal liabilities and/or negative publicity to the district. Examples of inappropriate usage include, but are not limited to:
 - The creation of, receipt, display or transmission of threatening, hostile, harassing, sexually and/or racially offensive language or any other communication that is deemed inappropriate
 - The creation of, receipt, display or transmission of certain information may violate software licensing laws and may constitute illegal downloading
 - Certain activities on the internet may qualify as impermissible personal business conducted from a DPS server, and/or
 - Certain activities can result in connection with inappropriate sites on the Internet allowing the district domain (e.g., john_doe@detroitk12.org) to be captured, possibly resulting in negative publicity
 - The Detroit Public Schools network must operate under the guidelines of the Child Information Protection Act (CIPA)

2.0 SCOPE

Detroit Public Schools has provided access to the Internet to its employees. As a provider of Internet use and email, Detroit Public Schools must ensure that the Internet is used in a way that is legal, safe, and secure so that Internet use can be a productive business tool. Any Detroit Public School employee or business partner representing Detroit Public Schools on the Internet must adhere to this policy.

3.0 POLICY

1. The Internet is a business tool for DPS. Access to the Internet is provided by DPS to its employees at a significant cost. That means DPS expects the Internet to be used for business-related purposes, which includes, but is not limited to, communication with customers and suppliers, to research relevant topics, and to obtain useful business information.
2. DPS requires that those employees and others who use DPS-provided internet access conduct themselves honestly and appropriately on the Internet, and that they comply with copyright laws, software licensing rules, property and privacy rights, and the prerogatives of others, just as in any other business dealings.
3. All existing DPS policies apply to conduct on the Internet, including, but not limited to DPS policies that address intellectual property protection, privacy and confidentiality rules, and policies on the misuse of DPS resources, information and data security. In addition to what any other DPS policy may require, this policy prohibits the transfer and/or dissemination of proprietary information, trade secrets, confidential documents or any other DPS privileged information via the Internet.
4. Detroit Public Schools does not extend nor imply a right to privacy in Internet usage or information exchanged on the Internet. As set forth in the Monitoring section below, DPS reserves the right to lawfully inspect and monitor internet usage and to examine any and all files stored in private areas of its network in order to assure compliance with DPS policies.
5. DPS may be required to preserve stored Internet information for extended or specified periods of time. Pursuant to State Department of Education, Bulletin No. 522, Revised, March 1997, DPS is required to retain documents that qualify as Business Office Records, Student Educational Records, Pupil Accounting Records, and other miscellaneous information for designated periods of time. If the information or files stored on the Internet fall into one of these categories and/or is required to be retained pursuant to Bulletin No. 522, then DPS may be required to archive such information.
6. The display of any kind of sexually explicit image or document on any DPS system is a violation of DPS policy, including but not limited to the DPS policy on sexual harassment. In addition, sexually explicit material may not be archived, stored, distributed, edited, or recorded using DPS network or computing resources.

7. DPS uses independently supplied software and data to identify inappropriate or sexually explicit Internet sites. DPS may block access from within its networks to all such sites of which DPS is aware. If a user finds that he or she was connected accidentally to a site that contains sexually explicit or offensive material, a user must disconnect from that site immediately, regardless of whether that site had been previously deemed acceptable by any screening or rating program. The reporting of Internet related concerns can be sent to info.protection@detroitk12.org.
8. DPS Internet facilities and computing resources must not be used knowingly to violate the laws and regulations of the United States or any other nation, or the laws and regulations of any state, city, province or other local jurisdiction in any material way.
9. An individual may not use the DPS-provided internet access to create, receive, display, transmit or download threatening, hostile or harassing information that is derogatory, defamatory, obscene, or offensive, or anything that may be perceived as harassment or disparagement based upon race, color, national origin, sex, sexual orientation, age, disability, or religious or political beliefs or that is deemed inappropriate based upon federal civil rights law, Michigan's Elliot Larsen Civil Rights Act, or other relevant law.
10. Any software or files downloaded via the Internet into the DPS network will become the property of the DPS. Any such files or software may be used only in ways that are consistent with the licenses and/or copyrights governing the software or files.
11. No individual may use DPS Internet facilities knowingly to download or distribute pirated software or data.
12. DPS Internet users may not establish a web site with links to or from the DPS site.
13. DPS Internet users are not authorized to purchase, acquire, or implement goods or services without prior approval from the Division of Technology and Information Systems.
14. No individual may use DPS Internet facilities to deliberately propagate a virus, worm, Trojan horse, trap-door program, or any other malicious code.
15. No individual may use the DPS Internet facilities knowingly to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.
16. Each individual using DPS internet facilities shall identify himself or herself honestly, accurately, and completely (including DPS affiliation and function where requested) when participating in chat rooms or newsgroups, or when setting up accounts on outside computer systems; however, only those agents, employees or officials who are duly authorized to speak to the media, to analysts, or in public gatherings on behalf of DPS may speak/write in the name of DPS to any newsgroup or chat room.

17. Employees and other internet users are reminded that chat rooms and newsgroups are public forums where it is inappropriate to reveal confidential DPS information, customer data, trade secrets, and any other material covered by existing DPS policies and procedures.
18. Use of DPS internet facilities to commit infractions, including but not limited to, the misuse of DPS assets or resources, sexual harassment, and misappropriation or theft of intellectual property is prohibited by DPS Policy 13.03 – Information Security.
19. Employees may use DPS Internet facilities for non-business research or browsing during mealtime or other breaks, or outside of work hours, provided that such use is in compliance with the DPS Internet Usage policy and other DPS policies.
20. Individuals with access to DPS Internet facilities may not use DPS Internet facilities to download entertainment software or games, or to play games against opponents over the Internet.
21. Individuals with access to DPS Internet facilities may not use DPS Internet facilities to download images or videos unless there is an explicit business-related use for the material.
22. Individuals who are not DPS employees, agents, or officials who gain access to the internet through DPS-provided internet facilities by way of an employee, agent or official of DPS are subject to the terms and conditions of this Internet Usage policy.
23. Web sites and/or internet addresses on the world-wide web that are identified by DPS as inappropriate, will be added to the dictionary or equivalent URL (Web page) filtering feature and an individual will not be allowed access to those sites.

4.0 MONITORING

DPS has the right to monitor usage of the DPS-provided Internet facilities by users, including but not limited to, reviewing a list of the sites accessed by an individual. The access to the Internet provided by DPS is for business purposes and the Internet should be used in accordance with the policy provisions set forth above. A DPS Internet user/DPS employee, agent or official should not have an expectation of privacy in the use of DPS-provided Internet facilities nor should they have an expectation of privacy in the information exchanged. Violation of the Internet policy or failure to comply with monitoring guidelines can lead to disciplinary and/or legal consequences.

Monitoring Approach

- DPS may monitor Internet usage on a periodic basis (daily, weekly, monthly, and bimonthly) and may generate Internet usage reports to ensure policy compliance.
- Violation of the terms of the above-referenced Internet Usage policy, provisions of other relevant DPS policies, federal, state or local laws will constitute non-compliance that can carry disciplinary or legal consequences, including but not limited to criminal prosecution.
- An employee may be notified of non-compliance with the Internet Usage policy, and/or provisions of other relevant DPS policies, federal, state, or local laws.

5.0 ISSUANCE OF REGULATIONS/STANDARD OPERATING PROCEDURES

The Chief Technology and Information Systems Officer is authorized to develop regulations and/or standard operating procedures to implement this policy.

6.0 FAILURE TO COMPLY

Non-compliance with this policy will be subject to management review and action in conformance with the DPS disciplinary policies and/or relevant legal action.

7.0 EXCEPTIONS

Any exceptions to this policy must be documented and approved by the DPS Chief Technology and Information Officer.

8.0 AGREEMENT

I, _____ (print name) have received a written copy of the DPS Internet Usage Policy, dated _____. I fully understand the terms of this policy and agree to abide by them. I realize that DPS security software may record for management use, the Internet address of any site that I visit and keep a record of any network activity in which I transmit or receive any kind of file. I acknowledge that any message I send or receive will be recorded and stored in an archive file for management use and/or review. I acknowledge that any violation of this policy could lead to disciplinary action up to and including dismissal and/or criminal prosecution or other legal action.

Signed