

Technology Acceptable Use Policy
REVISED Policy 3040
REVISED Policy 5150

Durham Public Schools (DPS) offers a county-wide area computer network with Internet access for students, teachers, and staff. Teachers and staff also have access to e-mail through the school system's network. The network and other school system technological resources provide opportunities to enhance instruction, appeal to different learning styles and meet the educational goals of the Board. Through the school system's technological resources, users can observe events as they occur around the world, interact with others on a variety of subjects, and acquire access to current and in-depth information. Access includes local, national and international connections to (1) libraries, companies, agencies and businesses; (2) discussion groups on a variety of subjects; (3) information news services; and (4) electronic mail communication.

Acceptable uses of technological resources are limited to activities that support learning and teaching, except when otherwise specifically authorized by the Superintendent in the best interest of the school system. Use of technological resources should be integrated into the educational program. Technological resources should be used in teaching the North Carolina Standard Course of Study and in meeting the educational goals of the Board. Teachers are encouraged to further incorporate the use of technological resources into their lesson plans.

This policy applies to all students and employees (including teachers, administrators, and staff), as well as any other users who are expressly authorized by the Durham Public Schools to use school system technological resources, including, but not limited to, Board of Education members, contractors, consultants, and temporary workers.

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. In addition, the Superintendent or Designee shall develop any other rules, procedures, forms or other guidance needed to implement this policy.

A. REQUIREMENTS FOR USE OF TECHNOLOGICAL RESOURCES

Durham Public Schools Board of Education realizes that today's 21st Century classrooms must use technology in order to achieve the district's academic goals for its students.

School system technological resources include, but are not limited to computers, interactive whiteboards, mobile devices, websites, networks, servers, the Internet, phones, copiers, facsimile machines, televisions and video-recorders, e-mail accounts, and licensed software.

Students are given the privilege to use the Internet along with the responsibility of using it properly. Students are responsible for exhibiting high standards of behavior in using the school system's technological resources as set forth in Board Policy 4301 Code of Student Conduct. Using the Information and Technology Essential Standards, students will be taught safe, ethical, and responsible uses of technological resources.

Staff members will instruct students in the correct use of these resources, and ensure that students read and understand the guidelines established by the district; however, the ultimate responsibility for a student's actions in using the technological resources rests with the student.

Failure to adhere to the requirements of this policy may result in disciplinary action, which may include immediate revocation of user privileges, suspension of access to school system computers, other disciplinary action, dismissal and/or appropriate legal action. Misuse or damage of any school system technological resource may result in disciplinary action and/or criminal prosecution under applicable state and federal law.

Employees should maintain the highest ethical behavior in using the Internet and should promote that behavior among students. When using technological resources in the classroom, instructional personnel shall:

1. Make every attempt to maintain the curricular focus of Internet use by locating and directing students toward sites on the Internet that support that focus;
2. Make reasonable efforts to supervise a student's use of the Internet during instructional time and ensure that it is in a manner that is appropriate to the student's age and circumstances of use;
3. Model and provide instruction in the ethical and appropriate use of the Internet in a proper school setting as provided in this policy; and
4. Follow the same criteria of Internet resources that are applicable to all instructional materials under the Board Policy 3015 Selection of Instructional Resources.

B. GUIDELINES FOR ACCEPTABLE USE: ALL USERS

1. School system technological resources are provided for school-related authorized purposes only. Acceptable uses of such technological resources are limited to responsible, efficient and legal activities that support teaching and learning. Use of school system technological resources for commercial or profit or for amusement or entertainment is prohibited. School system technological resources shall not be used for charitable endeavors without prior approval of the Superintendent or Designee. School system technological resources shall not be used for political purposes.
2. Under no circumstance may software purchased by the school system be copied for personal use. Users must obtain permission from the Technology Services Department prior to copying or loading school system software onto any computer, whether the computer is privately owned or is a Durham Public School System computer;
3. Students and employees must comply with all 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. All rules of the Code of Conduct apply to students' use of the Internet and other technological resources.
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, abusive 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, blogs or other forms of electronic communication, students must not reveal personally identifiable, private or confidential information, such as the home address, telephone number, credit or checking account information or social security number of themselves or fellow students. In addition, school employees will follow the guidelines of the Family Educational Rights and Privacy Act (FERPA), Board Policy 4200 Student Records and Board Policy 4207 Directory Information when publishing student information. Users also may not forward or post personal communications without the author's prior consent.
7. Users may not intentionally or negligently damage computers, computer systems, electronic devices, software, computer networks and/or data of anyone connected to the server or the Internet or waste computer resources. Users may not knowingly or negligently transmit computer viruses or self-replicating messages or deliberately try to degrade or disrupt system performance. The technology department provides antivirus software for all DPS-owned or leased computers. Users must not disable any antivirus programs from running on those computers.
8. Users may not create, download, or introduce entertainment software, 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 Technology Director or Designee. This prohibition pertains to freeware, shareware, copyrighted commercial and non-commercial software, and all other forms of software and files not directly related to the instructional and administrative purposes of the Durham Public School System.
9. 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.
10. Users are prohibited from using another individual's computer account. Users may not read, alter, change, block, execute or delete files or communications belonging to another user without appropriate authorization or the owner's express prior permission. In addition, employees shall not share or reveal their passwords or user IDs for any data system. All employees with access to NCWISE or other sensitive data are responsible for safeguarding their user IDs and passwords.
11. If a user identifies a security problem on a technological resource, he or she must immediately notify a supervisor without demonstrating the problem to other users. Unauthorized attempts to log onto any school system computer or the Durham Public School System network as a system administrator may result in cancellation of user privileges and/or additional disciplinary action. Any user identified as a security risk or having a history of problems with other computer system may be denied access.
12. 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.
13. School system technological resources may not be used to interfere with or disrupt other users, services, or equipment. Disruptions include, but are not limited to, distribution of unsolicited advertising; propagation of computer viruses; distribution of large quantities of information that may overwhelm the system; posting personal or private information about the user or other people on the Internet; arranging or agreeing to meet with someone the user has met on-line for purposes other than official school business; posting information that could be disrupting, cause damage, or endanger students or staff; and accessing chat-rooms or instant messaging software, unless for a valid educational purpose or official school business.
14. Using school system computers for illegal, harassing, or inappropriate purposes, or in support of such activities, is prohibited. Illegal activities are any violations of federal, state, or local laws and include,

but are not limited to, copyright infringement and/or illegal file sharing; committing fraud; threatening another person; or intentionally engaging in communications for the purpose of abusing, annoying, threatening, terrifying, harassing, or embarrassing another person. 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 (1) have the purpose or effect of creating an intimidating, hostile or offensive environment; (2) have the purpose or effect of unreasonably interfering with an individual's work or school performance, or (3) interfere with school operations. Inappropriate use is any violation of other provisions of this policy and includes, but is not limited to, using another person's ID or password; plagiarizing; accessing, producing, storing, posting, sending, displaying, or viewing inappropriate or offensive material, including pornographic, obscene, discriminatory, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, or sexually suggestive language or images, or images of exposed private body parts; and accessing material advocating illegal acts or violence, including hate literature.

C. INTERNET SAFETY

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. 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. Employees may have a different level of blocks or filters based on district guidelines.

D. PRIVACY

Durham Public School System electronic information resources, the Internet, and use of e-mail are not inherently secure or private. No right of privacy exists in the use of technological resources. Users shall have no expectation of privacy while using school system technological resources. Users should not assume that files or communications created or transmitted using school system technological resources or stored on servers or hard drives of individual computers will be private. 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 online activities of individuals who access the Internet via a school-owned computer. The Board reserves the right to take appropriate disciplinary action based on the user's inappropriate or illegal use or use that is in violation of this policy. Communications relating to or in support of illegal activities will be reported to the appropriate authorities. Information in electronic messages is not anonymous and is subject to disclosure to third parties under state and/or federal law in certain circumstances.

E. 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.

1. Students

Though school personnel generally do not monitor students' Internet activity conducted on non-school system computers during non-school hours, when the student's online 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 Board Policy 4301 Student Code of Conduct.

2. Employees

Employees are to maintain an appropriate relationship with students at all times. Employees are encouraged to block students from viewing personal information on employee personal websites or online networking profiles in order to prevent the possibility that students could view materials that are not age-appropriate. Employees may not use personal web sites or online networking profiles to post information in an attempt to communicate with students in their roles as school system employees. If an employee creates and/or posts inappropriate content on a website or profile or engages in any direct communication with students, parents, supervisors or co-workers (whether by email, instant messaging, or other digital media) and it has a negative impact on the employee's ability to perform his or her job as it relates to working with students, the employee will be subject to discipline up to and including dismissal. This section applies to all employees, volunteers and student teachers working in the school system.

F. EMPLOYEE PERSONAL USE

The Board expects that employee use of technological resources will be related to the school system's goals of educating students and/or conducting school system business. The Board recognizes, however, that some personal use is inevitable, and that incidental and occasional personal use that is infrequent or brief in duration is permitted so long as it occurs on personal time, does not interfere with the employee's work or school system business, and is not otherwise prohibited by Board policy or regulations, Durham Public School System procedures, or applicable law.

G. CARE OF PROPERTY

Users of Durham Public School System computers are expected to respect school system property and be responsible in using the equipment. Users are to follow all instructions regarding maintenance or care of the equipment. Users may be held responsible for any loss or damage caused by intentional or negligent acts in caring for computers while under their control. The school system is responsible for any routine maintenance or standard repairs to school system computers. Users are expected to timely notify the Technology Services Department of any need for service.

H. NO WARRANTIES

The Durham Public School System makes no warranties of any kind, whether express or implied, for the electronic information resources it is providing. The board will not be responsible for any damages suffered by users, including loss of data resulting from delays, non-delivery, service interruptions, or any other cause. The board will not be responsible for any claims, losses, damages, costs, or other obligations arising from the unauthorized use of school system electronic information resources. Use of any information obtained via the Internet is at the user's risk. The board specifically denies any responsibility for the accuracy or quality of information obtained through its service. Users are responsible for any losses sustained by the Durham Public School System resulting from the user's intentional misuse of the school system's electronic information resources.

I. APPLICATION OF PUBLIC RECORDS LAW

All information created or received for work purposes and stored on or contained in the school system's computer resources or electronic data files is subject to public disclosure unless an exception to the Public Records Law applies. This information may be purged or destroyed only in accordance with the applicable records retention schedule and the State Division of Archives regulations.

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

Children's Internet Protection Act Cross Reference: Board Policy 4301; Code of Student Conduct; Board Policy 3015 Selection of Instructional Resources; Board Policy 3060 Copyright.

Adopted Effective: January 24, 1996

Revised Effective: April 24, 2011

Revised Effective: December 13, 2001

Revised Effective: July 1, 2011