

SCHOOL DISTRICT OF UPPER DUBLIN

TITLE: ACCEPTABLE USE OF
DISTRICT INFORMATION AND
TELECOMMUNICATIONS
RESOURCES BY STUDENTS

ADOPTED: June 1, 2004

REVISED:

<p>1. Purpose</p> <p>2. Definitions</p> <p>3. Guidelines</p>	<p style="text-align: center;">815. ACCEPTABLE USE OF DISTRICT INFORMATION AND TELECOMMUNICATIONS RESOURCES BY STUDENTS</p> <p>It is Board policy that the use of any and all information and telecommunications resources accessed through the Upper Dublin Network Services (UDNS) will be legal, in adherence with standards of the District and the community, and solely for educational purposes consistent with the curricular goals of the District.</p> <p>The term educational purpose includes use of the system for classroom activities, professional or career development, limited high-quality self-discovery activities, and administrative application.</p> <p>UDNS is the title of the District's Network Services.</p> <p><u>General</u></p> <p>These guidelines shall apply to all users who obtain access privileges to networks and telecommunications systems, which are entered via equipment and access lines housed, operated or maintained by or for the District. In addition, these policies shall, where appropriate, be applicable to the use of all District information and telecommunications resources, whether connected to an electronic network or operated on a "stand alone" basis, as well as access to information networks and services provided to the user by or through the District, regardless of the location or ownership of the equipment through which a network or service is accessed.</p> <p>Accounts for accessing all information and telecommunications resources and electronic networks maintained by or for the District (internal networks), or other networks which may be accessed through the District network, will be provided to users solely for the purpose of aiding education and research.</p> <p>The use of UDNS is a privilege, which may be revoked by the network administrators at any time for abusive conduct or violation of the conditions of this policy or the administrative regulations developed in support of this policy.</p>
--	---

815. ACCEPTABLE USE OF DISTRICT INFORMATION
AND TELECOMMUNICATIONS RESOURCES BY STUDENTS - Pg. 2

The UDNS will not warrant what functions of the system and network will meet any specific requirements, or that it will be error free or uninterrupted; nor shall it be liable for any direct, incidental, or consequential damages sustained or incurred in conjunction with the use, operation or inability to access or use the system or network, including the loss of data, information or anything else of value which the user seeks to maintain or derive through the network. The District shall not be liable for any damage incurred due to harmful programs or materials (including computer viruses), which may be accessible or propagated through networks such as UDNS.

Electronic mail (E-mail) accounts and other forms of electronic communication provided by or through UDNS are not guaranteed to be private. Network administrators may access mail and other forms of communication at any time, and E-mail software may misdirect messages. Users should be aware of these limitations when corresponding or communicating with others.

Additionally, when a student is logged on to UDNS, whether at a District facility or remotely, District employees have the ability to view what appears on the student's monitor through a feature called "shadowing." District employees will only use this feature for legitimate educational purposes, including ensuring that UDNS is only being used for educational purposes. Authorized District employees, including Technology Management Services personnel, may use the shadowing feature without notice at any time.

Posting personal communications to public spaces without the original author's prior consent is prohibited. However, messages accessible in public forum may be copied in subsequent communications, as long as proper attribution is given.

Use of the network or its hardware or software components for any activities considered criminal under local, state, or federal law is prohibited, including knowledgeable vandalism of, destruction of, tampering with or unauthorized entry into computers, files or software. The District will cooperate fully with local, state, and federal officials in any investigation conducted concerning or related to alleged illegal activities of any individuals misusing the District's system.

Parental Notification and Responsibility

The Superintendent shall implement a program, which educates students about the risks and consequences associated with the use of the UDNS. The District will notify the parent or legal guardian about the District system and the policies governing its use. A parent or legal guardian must sign a Student Internet Permission Form to allow their student to have an individual account. Parents or legal guardians may request alternative activities for their child(ren) that do not require Internet access.

815. ACCEPTABLE USE OF DISTRICT INFORMATION
AND TELECOMMUNICATIONS RESOURCES BY STUDENTS - Pg. 3

The District Acceptable Use Policy contains restrictions on accessing inappropriate material. There is a wide range of material available on the Internet, some of which may not fit with the particular values of students' families. The District will use appropriate blocking software. However, no filtering software is 100% effective. The District reserves the right to monitor and censor the content of all materials that students might access on school computer systems and equipment, and will make every attempt to see that inappropriate content is filtered. The District reserves the right to prohibit any web site content accessed by users. However, it is not practically possible for the District to monitor and enforce a wide range of social values in student use of the Internet. Further, the District recognizes the parents or legal guardians bear primary responsibility for transmitting their particular set of family values to their children. The District will encourage parents or legal guardians to specify to their child(ren) what material is and is not acceptable for this child(ren) to access through the District system, within the parameters of this policy.

The District will provide students and parents or legal guardians with guidelines for student safety while using the Internet.

Parents or legal guardians are responsible for monitoring their student's use of the Internet when they are accessing the system from home.

District Limitation of Liability

The District makes no warranties of any kind, either express or implied, that the functions or the services provided by or through the District system are error-free or without defect. The District will not be responsible for any damage users may suffer, including but not limited to, loss of data or interruptions of service. The District is not responsible for financial obligations arising through the unauthorized use of the system. Users will indemnify the District against any damage caused by the user's inappropriate use of the system.

Due Process

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

In the event there is an allegation that a student has violated the District Acceptable Use Policy, the student will be provided with notice of the alleged violation and be given an opportunity to present an explanation.

815. ACCEPTABLE USE OF DISTRICT INFORMATION
AND TELECOMMUNICATIONS RESOURCES BY STUDENTS - Pg. 4

Disciplinary actions will be tailored to meet specific concerns related to the violation and to assist the student in gaining the self-discipline necessary to appropriately use an electronic network.

All student accounts will be revoked immediately following withdrawal from the District.

The technology department or Technology Coordinator may revoke the account privileges of a guest user by providing notice to the user. Guest accounts not active for more than thirty (30) days may be removed, along with the user's files, without notice to the user.

Search and Seizure

System users have no privacy expectation in the contents of their personal files on the District system.

Routine maintenance and monitoring of the system may lead to discovery that the user has or is violating the District Acceptable Use Policy, the discipline policy, or the law.

An individual search may be conducted if there is reasonable suspicion that a user has violated the law or the District policies. The nature of the investigation will be reasonable and in the context of the nature of the alleged violation.

System users have no privacy expectation regarding what appears on their screen at any given time in light of the "shadowing" feature, which enables authorized District employees and contract employees to view what appears on a user's monitor when the user is logged on to UDNS.

Copyright

The Board affirms that respect for personal property, whether tangible or intangible, is vital to maintaining a stable learning and working environment. The Superintendent will establish and promulgate copyright procedures for student users.

Students of the District are expected to follow copyright law and the copyright procedures established by the Superintendent and Board policy. Any willful infringement will be punished in accordance with the student disciplinary code. Students who willfully infringe the copyrights of others will be reported to the appropriate authorities and may be subject to criminal or civil penalties.

815. ACCEPTABLE USE OF DISTRICT INFORMATION
AND TELECOMMUNICATIONS RESOURCES BY STUDENTS - Pg. 5

Users will not plagiarize. Teachers will instruct students in appropriate research and citation practices.

Student users will not install software unless the software has been legally obtained and only into the specified, approved computers. Downloading or loading software will require permission of the Network Administrator. Technology staff will remove unlicensed software programs without advance notice to the user who installed the program.

Establishment of Web Sites

1. District Web Site – The District may establish a web site and develop web pages that present information about the District. The Educational Technology Coordinator will be responsible for managing the District web site.
2. School or Class Web Pages – Schools and classes may establish web pages that present information about the school or class activities. The building principal will designate an individual to be responsible for managing the school web site under the supervision of the computer coordinator. Teachers will be responsible for maintaining their class sites.
3. Student Web Pages – With the approval of the Activity Advisor, students may establish individual school-related web pages. The Activity Advisor will establish a process and criteria for the establishment and posting of material, including linking to other sites, on these pages. Material presented in the student’s web site must be related to the student’s educational and career preparation activities. 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 School District of Upper Dublin.”
4. Extracurricular Organization Web Pages – With the approval of the computer coordinator, extracurricular organizations may establish web pages. The computer coordinator will establish a process and criteria for the establishment and posting of material, including pointers to other sites, on these pages. Material presented on the organization web page must relate specifically to organization activities and will include only student-produced material. 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 School District of Upper Dublin.”

815. ACCEPTABLE USE OF DISTRICT INFORMATION
AND TELECOMMUNICATIONS RESOURCES BY STUDENTS - Pg. 6

5. Written permission from both the parent/guardian and the student must be obtained prior to placing any student photographs, artwork, writing, or other projects on a web site. No personal contact information about the child, such as home address, phone number, or e-mail address will be given. The work will appear with a copyright notice prohibiting the copying of such work with express written permission. In the event that anyone requests such permission, those requests will be forwarded to the parent or guardian. All such work will be removed from the web site at the end of the current school year.

User Responsibilities

1. Personal Safety

- a. Users will not post personal contact information about themselves or other people. Personal contact information includes address, telephones, school address, work address, etc.
- b. Student users will not agree to meet with someone they have met online without their parent or legal guardian's approval and participation.
- c. Student users will promptly disclose to their teacher or other school employee any message they receive that is inappropriate or makes them feel uncomfortable.

2. Illegal Activities

- a. Users will not attempt to gain unauthorized access to the District system or to any other computer system through the District system, or go beyond their authorized access. This includes attempting to log in through another person's account or access another person's files. These actions are illegal, even if only for the purpose of "browsing."
- b. Users will not make deliberate attempts to disrupt the system performance or destroy data by spreading computer viruses or by any other means. These actions are illegal.
- c. Users will not use the District system to engage in any other illegal act, such as arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, threatening the safety of a person, etc.

815. ACCEPTABLE USE OF DISTRICT INFORMATION
AND TELECOMMUNICATIONS RESOURCES BY STUDENTS - Pg. 7

System Security

1. Users are responsible for the use of their individual account 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.
2. Users will immediately notify the technology department or computer coordinator if they have identified a possible security problem. Users may not search for security problems; this may be construed as an illegal attempt to gain access.
3. Users will avoid the inadvertent spread of computer viruses by following the District virus protection procedures. All diskettes must be run through a virus check prior to use on any District system.
4. Users will not introduce, remove or copy any application or operating system programs on any District system without prior approval from the computer coordinator.
5. No user will connect or disconnect any device from any District network system without prior approval from the computer coordinator.

Access to Inappropriate Material

1. Access to Inappropriate Material
 - a. Users will not use the District system to access material that is profane or obscene (pornography), that advocates illegal acts, or that advocates violence or discrimination towards other people (hate literature). For students, a special exception may be made for hate literature if the purpose of such access is to conduct research and access is approved by both the teacher and the parent or legal guardian.
 - b. If a user inadvertently accesses such information, they should immediately disclose the inadvertent access to their teacher in a manner specified by their school. This will protect other users from accessing the same information, and the users against an allegation that they have intentionally violated the Acceptable Use Policy. This information should not be disclosed to other users, as such action constitutes a violation of policy.

815. ACCEPTABLE USE OF DISTRICT INFORMATION
AND TELECOMMUNICATIONS RESOURCES BY STUDENTS - Pg. 8

2. Commercial Purposes

- a. Users will not use the District system for commercial purposes. **Commercial purposes** are defined as offering or providing, soliciting or requesting goods or services for personal use. District acquisition policies will apply to the District purchase of goods or services through the system.

3. Political Activities

- a. Users will not use the District system for political lobbying. Students may use the system to communicate with their elected representatives and to express their opinion on political issues.

Actions Resulting From Misuse

1. Deliberate and/or negligent abuse of the network, computing resource, or any other District resource could lead to disciplinary action. Any such action will be subject to applicable policies and procedures established by the District.

Offenders may also be subject to criminal prosecution. Under Pennsylvania law it is a felony punishable by fine up to \$15,000.00 and imprisonment of up to seven (7) years for any person to access, alter, or damage any computer system, networking, software, or database, or any part thereof, with the intent to interrupt the normal functioning of an organization. Knowingly and without authorization, disclosing a password to a computer system, network, etc., is a misdemeanor punishable by a fine of up to \$10,000.00 and imprisonment of up to five (5) years, as is intentional and unauthorized access to a computer, or alteration of computer software.