

**DOWNINGTOWN AREA SCHOOL DISTRICT
SCHOOL BOARD POLICYU
SECTION: OPERATIONS**

815. ACCEPTABLE USE POLICY

POLICY 815 – ACCEPTABLE USE POLICY (AUP)
POLICY 815.1 WEB SITE RELEASE

STUDENT RELEASE

Acceptable Use Policy (AUP) Agreement (for students to sign):

I understand and will abide by the AUP Agreement, Board Policy #815. I further understand that any violation of the regulations is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, school disciplinary action and appropriate legal action may be taken.

STUDENT NAME: (please print)

GRADE:

STUDENT SIGNATURE:

DATE:

PARENT RELEASE

AUP Agreement and Student Release Form (for Parent or Guardian to sign)

As the parent or guardian of this student, I have read Policy 815 –AUP and Policy 815.1 Web Site

APPROVE

DISAPPROVE

My child may have access to the District's computers, systems, and Wide Area Network, including the Internet.

PARENT RELEASE

Release of Student Information on District/school websites or print media:

Downingtown Area School District has established websites at both the District and building levels. On occasion, the District and/or schools may wish to post or publish in print student work, including photographs and information such as student name, grade level, and school. **Under no circumstance will the following personal information be displayed for public access: home address, home phone number, or home email address.**

APPROVE

DISAPPROVE

EXTERNAL - Newspaper/TV/District/School photograph and video clip publication

Permission for my child to be part of photographs or video clips of school related activities news or publicity

INTERNAL - District/School photograph and video clip publication

Permission for my child to be part of school related photographs or video clips (i.e. school yearbooks, class photos etc.)

DISTRICT WEBSITES - School and District photographs

Permission for my child to be included in photographs published on our school and/or district website.

PARENT RELEASE

APPROVE

DISAPPROVE

Student Directory

Permission for my child's name, address, telephone number, parent's name, teacher and grade level to be included in the school directory that is sent home to each family.

**PARENT / GUARDIAN NAME:
(Please print)**

PARENT / GUARDIAN SIGNATURE:

DATE:

DOWNINGTOWN AREA SCHOOL DISTRICT
SCHOOL BOARD POLICY
SECTION: OPERATIONS

1
2 1. PURPOSE
3

4 Downingtown Area School District provides various technologies to its staff and students
5 that are to be used as learning resources to educate and to inform. Use of the District's
6 computers and Wide Area Network to access the Internet and electronic communications
7 require students and staff to think critically, analyze information, write clearly, and use
8 problem-solving skills, and hone computer and research skills that embody a 21st Century
9 citizen. Use of these tools encourages an attitude of lifelong learning and offers an
10 opportunity for students to participate in distance learning activities, ask questions of and
11 consult with experts, communicate with other staff members, students and individuals, and
12 locate materials to meet educational and personal information needs. Students and staff
13 should take responsibility for their own use of District computers and the Wide Area
14 Network avoiding instances that are not consistent of an educational environment. The
15 Board establishes that the used of the Wide Area Network, the Internet, the District
16 computers and the District technology is a privilege, not a right; inappropriate,
17 unauthorized, and/or illegal use will result in the cancellation of those privileges and
18 appropriate disciplinary action as stated in this policy and in the Student Discipline Policy
19 (#218).

20
21 2. AUTHORITY
22

23 The Board of Directors and Downingtown Area School District recognizes the need to
24 establish a policy for students and staff uses of Downingtown Area School District
25 computers and the Wide Area Network that are consistent with the educational goals of the
26 school District. The Wide Area Network consists of two parts: the internal network which
27 promotes, stimulates, and supports educational endeavors both on and off the school
28 campus, and Internet access which enables students and staff to utilize the vast wealth of
29 resources available globally.

30
31 The school District makes no warranties of any kind, whether expressed or implied, related
32 to the use of District computers and computer systems, including access to the Internet and
33 electronic communications services. Providing access to these services does not imply
34 endorsement by the District of the content, nor does the District make any guarantee as to
35 the accuracy or quantity of information received. The school District shall not be responsible
36 for any damages, losses or costs a student or staff member suffers in using the Internet and
37 electronic communications. This includes loss of data and service interruptions.

38
39 In compliance with the Children's Internet Protection Act (CIPA), the Downingtown Area
40 School District has implemented content filtering and/or blocking software to restrict access
41 to Internet sites containing pornography, obscene depictions, or other materials harmful to
42 minors under 18 years of age. Additionally, content and spam filtering software is applied to
43 all email correspondence on Downingtown Area School District's electronic mail system.
44 The Superintendent may authorize the Director of Technology to disable the technology
45 protection measures to enable Internet access for bonafide research or other lawful
46 purposes.

47
48 District computers, computer systems, and the Wide Area Network are owned by the
49 District and are intended for educational purposes at all times. Students and staff shall

DOWNINGTOWN AREA SCHOOL DISTRICT
SCHOOL BOARD POLICY
SECTION: OPERATIONS

1 have no expectation of privacy when using the Wide Area Network or electronic
2 communications, including email and instant messaging. The District reserves the right to
3 monitor, inspect, copy, review and store (at any time and without prior notice) all usage of
4 District computers and computer systems, including all Internet and electronic
5 communications access and transmission/receipt of materials and information. Any party
6 who uses the District's technology systems to transmit or receive communications shall be
7 deemed to have consented to having the content of any such communications reviewed by
8 the District. All material and information accessed/received through District computers
9 and computer systems shall remain the property of the school District. Downingtown Area
10 School District's communication systems work in such a way that messages will be
11 preserved for a period of time as computer files on centrally administered disks and at
12 system back-up locations, even if they have been deleted or downloaded off the user's
13 computer.

14
15 **3. ACCEPTABLE USE**

16
17 No policy can cover every possible specific case of acceptable and unacceptable behavior in
18 computer use; the key is to understand that the same laws, regulations, and customs which
19 govern behavior in civilized life also apply to the computer usage. What follows is a general
20 outline which delineates the principles of the Downingtown Area School District's
21 acceptable use policy; it is up to the user to read these rules, understand them, and be able
22 to apply them to the conditions of his or her computer use. These regulations apply to the
23 use of individual computers, school networks (a network is defined as a number of
24 computers and electronic tools that are connected to each other for the purpose of
25 communication and data sharing), school e-mail, internet use, and internet e-mail.

26
27 **A) PERSONAL INFORMATION**

28 Accessing or revealing unauthorized personal information is prohibited by
29 students and staff unless express written permission is granted. Personal
30 information may include, but is not limited to, such information as home
31 address, telephone number, credit card number, and social security number.
32 Student users should never agree to meet with someone they meet on-line
33 without a parent/guardian's approval.

34
35 **B) SYSTEM SECURITY**

36 Security on District computer systems is a high priority. The Superintendent
37 or his/her designee shall be responsible for implementing procedures and
38 technologies that will enable the appropriate and safe use of the Internet and
39 other network resources. Furthermore, students and unauthorized staff,
40 unless expressly permitted, who identify a security problem while using the
41 Internet or electronic communications must immediately notify a system
42 administrator. Students should not demonstrate the problem to other users.
43 Students logging on to the Internet or electronic communications as a system
44 administrator are prohibited. Students and staff should not:

- 45 • Use another person's password or any other identifier
- 46 • Gain or attempt to gain unauthorized access to District computers or
47 computer systems
- 48 • Read, alter, delete or copy or attempt to do so, electronic
49 communications of other system users

**DOWNINGTOWN AREA SCHOOL DISTRICT
SCHOOL BOARD POLICYU
SECTION: OPERATIONS**

- Trespass in another user’s folders, work, and files

C) **PROHIBITED ACTIVITIES**

a. **ELECTRONIC VANDALISM**

Vandalism is defined as any malicious attempt to harm or destroy data of another user, Internet, or other networks; this includes but not limited to uploading or creating computer viruses. These actions are felonies in the Commonwealth of Pennsylvania (Title 18, Section 7611 Unlawful Use of the computer).

b. **ELECTRONIC TRESPASS**

Trespass is defined as attempting to circumvent data protection schemes or uncover security loop holes by probing network servers, computers, or systems in order to exploit vulnerabilities. Students and staff are only permitted to utilize those resources assigned. A system need not prevent unauthorized access for trespassing to occur. These actions are felonies in the Commonwealth of Pennsylvania (Title 18, Section 7615 Computer trespass) even if only for the purpose of “browsing”.

c. **INSTALLATION OF UNAUTHORIZED SOFTWARE**

Students and Staff may not install software on the District’s computers, including servers, without the consent of the building principal and the Director of Technology.

d. **CYBER BULLYING**

Students or staff may not engage in “Cyberbullying.” Cyberbullying is defined as “willful and repeated harm inflicted through the medium of electronic media.” It may involve:

- sending mean, vulgar or threatening messages or images
- posting sensitive, private information about another person
- pretending to be someone else in order to make that person look bad
- intentionally excluding someone from an online group

e. The Board also establishes that the following materials in addition to those stated in law, are inappropriate for access: sites with pornography or nudity, sites which promote violence, sites which provide information on performing criminal acts, sites which promote or provide information on the use of illegal drugs, sites advocating, promoting discrimination or intolerance, sites which promote gambling, sites which promote possession or the use of illegal weapons, and any other site that may be deemed inappropriate in the future.

D) **ELECTRONIC COMMUNICATIONS**

The District provides staff and students electronic communication resources to support its work of teaching, scholarly research, and public service. The District will make reasonable efforts to maintain the integrity and effective

DOWNINGTOWN AREA SCHOOL DISTRICT
SCHOOL BOARD POLICYU
SECTION: OPERATIONS

1 operation of its electronic mail systems, but users are advised that those
2 systems should in no way be regarded as a secure medium for the
3 communication of sensitive or confidential information. Because of the nature
4 and technology of electronic communication, the District can assure neither
5 the privacy of an individual user's use of the District's electronic mail
6 resources nor the confidentiality of particular messages that may be created,
7 transmitted, received, or stored thereby. Furthermore, the contents of
8 electronic communications can be considered public record and may be
9 disclosed without permission of the user.

10
11 a. EMAIL

12 It is permissible to use the company email system for incidental
13 personal purposes. This does not include uses requiring substantial
14 expenditures of time, uses for profit or uses that would otherwise
15 violate District policy with regard to employee time commitments or
16 District equipment. Other prohibited uses of electronic mail include,
17 but are not limited to:

- 18 i. Sending copies of documents in violation of copyright laws
- 19 ii. Use of electronic mail to harass or intimidate others or to
20 interfere with the ability of others to conduct District business
- 21 iii. Use of electronic mail systems for any purpose restricted or
22 prohibited by laws or regulations
- 23 iv. "Spoofing," i.e., constructing an electronic mail communication
24 so it appears to be from someone else
- 25 v. Attempting unauthorized access to electronic mail or
26 attempting to breach any security measures on any electronic
27 mail system, or attempting to intercept any electronic mail
28 transmissions without proper authorization

29
30 b. INSTANT MESSAGING

31 Instant Messaging is available for staff only. Users will follow all
32 rules and regulations that apply to email, including archival.

33
34 c. ETIQUETTE

35 You are expected to abide by the generally accepted rules of network
36 etiquette. These include but are not limited to the following:

- 37 i. Be polite. Do not get abusive in your messages to others.
- 38 ii. Do not use vulgarities or any other inappropriate language.
- 39 iii. Do not interfere with or disrupt other network users, networks
40 services or network equipment.
- 41 iv. Do not change the configuration of any workstation.

42
43 E) PLAGIARISM AND COPYRIGHT

44 Students and staff shall not plagiarize works, including items that are
45 accessible on the Internet. Plagiarism is taking the ideas or writings of
46 others and presenting them as if they were yours. Students and staff shall
47 respect the rights of copyright owners. Copyright infringement occurs when
48 one inappropriately reproduces a work that is protected by a copyright. If a
49 work contains language that specifies appropriate use of that work, follow the

DOWNINGTOWN AREA SCHOOL DISTRICT
SCHOOL BOARD POLICYU
SECTION: OPERATIONS

ADMINISTRATIVE GUIDELINES FOR ACCEPTABLE USE POLICY

E-Mail Guidelines

Email messages can sometimes be records that are subject to review with sufficient justification. They may be subject to Pennsylvania Right to Know Act if they were produced, collected, received or retained in pursuance of law or in connection with the transaction of public business (rarely the case with student e-mail).

Administrators overseeing the District's disciplinary processes may rule that email or other files are evidence that may be reviewed as part of investigations. Although files might have been downloaded or email messages might have been deleted, Downingtown Area School District's delivery systems work in such a way that messages may be preserved for a time as computer files on centrally administered disks and at system back-up locations, so the capacity to control if and where copies exist is not absolute.

District procedures allow the Director of Technology or designee to view and modify any files, including email messages, in the course of diagnosing or resolving system problems and maintaining information integrity. The Director of Technology or designee, as part of their jobs, are expected to treat any such information on the systems as confidential. However, if the Director of Technology or designee come across information that indicates a violation of this policy or illegal activity, he or she will report the discovery to appropriate authorities.

Other important tips related to e-mail:

- Email messages become the possession of the receiver. They can be redistributed easily by recipients, and rules of disclosure by their systems apply to received mail. When in doubt, double-check the addresses of your intended recipients.
- Think before you send e-mail—once sent it is almost impossible to keep email messages from reaching their destinations.
- Realize that secure passwords provide good but not complete assurance of the privacy of your email messages. When the privacy of a message is of the utmost importance, only a person-to-person conversation may be sufficiently secure.
- Delete messages that should not be preserved.
- Never send or forward chain mail, whether it promises fame and fortune, or even supposed donations for a sick child. In virtually every known case, the claims made by such messages are untrue. This constitutes a violation as a waste of computing resources and a nuisance and often offends recipients.
- Do not pass on unconfirmed rumors—especially about viruses—because they often only cause needless panic. You can check a list of well-known virus hoaxes at <http://www.snopes.com> as well as other well-known hoaxes that

DOWNINGTOWN AREA SCHOOL DISTRICT
SCHOOL BOARD POLICYU
SECTION: OPERATIONS

1 may not involve computers but about which you may receive information via
2 e-mail.

- 3
4 • Do not open or execute attachments about which you have any question, even
5 if they appear to be coming from a friend. Attachments have become an
6 increasingly popular way of automatically distributing viruses, and your
7 friend may not even know that his or her email account is being used for that
8 purpose.
9
- 10 • Configure your email program so that attachments are only opened when you
11 choose to open them.
12
- 13 • If you are sending attachments, include personalized text and specific
14 references to the attachment (i.e., "Attached, in Word format, is my paper on .
15 . .") to help the recipient know that the message and attachment are indeed
16 from you.
17

DOWNINGTOWN AREA SCHOOL DISTRICT
SCHOOL BOARD POLICY
SECTION: OPERATIONS

ADMINISTRATIVE GUIDELINES FOR ACCEPTABLE USE POLICY

1
2
3
4 Violation Protocol

5
6 When any District administrator/supervisor, staff member or student has evidence that an
7 administrator, student or staff member has violated the Acceptable Use Policy following
8 guidelines shall be applied:

- 9 • The building principal/supervisor shall complete the Technology Incident
10 Report.
11 • The building principal/supervisor shall promptly report the incident within 24
12 hours to the Director of Technology or his/her designee.
13 • The building principal/supervisor shall confiscate all personal storage devices
14 and conduct an investigation into the alleged activity.
15 • Based upon the investigation, the building principal/supervisor may report
16 the administrator, student or staff member to law enforcement officials.
17 • The Superintendent or his/her designee may recommend expulsion of the
18 student to the Board or terminate administrator or staff employment. Such
19 expulsion shall be given in conformance with formal due process proceedings
20 required by law.
21 • Any employee who is in violation of this policy or exhibits unlawful use of the
22 District's resources be subject to disciplinary action up to and including
23 discharge.
24

25 If the student is expelled for violating the Acceptable Use Policy, upon return to school, the
26 student shall be subject to monitoring and/or have restricted network access.
27

28 In the event that a user inadvertently accesses material that is inappropriate or prohibited
29 as defined by Board Policy #815, the user should immediately cease operation of the
30 computer and the network resource and contact the nearest superior, who in turn shall
31 immediately contact the Director of Technology for further instructions.
32

33 Alleged Acceptable Use Violation Protocol

- 34 1. Upon notification of a possible violation, The Department of Technology will
35 lock the administrator's, student's or staff member's network accounts and
36 any personal storage devices are surrendered for inspection.
37
38 2. Witness(es) and/or the student(s) or staff being accused write and sign their
39 account(s). Parents of student witness(es) are contacted and asked if they can
40 support their child.
41
42 3. The Director of Secondary Education or the Director of Elementary Education
43 or applicable Supervisor will be contacted with the results of the
44 investigation.
45
46 4. If the investigation results show that the student or staff member has not
47 committed an Acceptable Use Violation the student or staff member has
48 his/her network account privileges reinstated.

DOWNINGTOWN AREA SCHOOL DISTRICT
SCHOOL BOARD POLICYU
SECTION: OPERATIONS

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32

5. If the investigation results show that the student or staff member has committed an Acceptable Use Violation, the following will occur:
- A. The acts and/or threats will be reported to the police.
 - B. Any employee who is in violation of this policy or exhibits unlawful use of the District's resources will be subject to disciplinary action up to and including discharge.
 - C. If a student is found to be in violation of this policy or exhibits unlawful use of the District's resources, crisis intervention will be contacted to meet with administrators, parent(s) and students to arrange for psychiatric evaluation to determine student's danger to others and/or himself/herself.
 - D. Student will remain out of school until psychiatric evaluation is obtained.
 - E. Crisis intervention will make a referral to a SAS counselor for monitoring.
 - F. The Director of Secondary Education or the Director of Elementary Education, as applicable, and Building Administrator will make a decision with regard to additional disciplinary action.

ADOPTED: 01/08/1997
REVIEWED: 03/08/2000
REVISED: 08/13/2008

DOWNINGTOWN AREA SCHOOL DISTRICT
SCHOOL BOARD POLICY
SECTION: OPERATIONS

815.1 WEB SITE

1
2
3 1. PURPOSE

4 In a continuing effort to fulfill the mission of the Downingtown Area School District by
5 preparing students to meet the challenges of a global society, the School Board endorses and
6 promotes the establishment of web sites as a valid format for communication. Web sites
7 will increase intra-district and community communication and enable the District to
8 communicate with people throughout the world.
9

10 2. AUTHORITY

11 The District may establish web sites and develop web pages at the District, building,
12 classroom, teacher, and student levels in order to communicate information, programs, and
13 activities that support the mission and strategic plan of the District. The Superintendent of
14 the District through the Director of Technology will oversee web site development,
15 implementation, and evaluation. Within each physical originating site (*i.e.* school building,
16 District office, etc.), the building principal or an administrator appointed by the
17 Superintendent, will approve all web content and site activities, will ensure teachers and
18 support staff have proper training, and will orient and enforce the guidelines and
19 responsibilities of this policy.
20

21 3. PUBLIC AND SECURE SITES

22 The district differentiates between secure-areas of the internet and non-secure areas.
23 Secure sites can and will contain information about students and staff that is not available
24 to the general public. The district defines a secure area of the web to mean a site that is
25 password protected and has either Transport Layer Security or Secure Sockets Layer
26 protocols in place to secure the transmission of the data across the internet. Transport
27 Layer Security (TLS) or Secure Sockets Layer (SSL), are cryptographic protocols that
28 provide secure communications on the Internet for such things as web browsing, e-mail,
29 Internet faxing, instant messaging and other data transfers.
30

31 4. RESPONSIBILITIES

32 It is the responsibility of the Superintendent or designee to annually communicate, in
33 writing, the policies of the District for web site use.
34

35 A. ESTABLISHMENT

- 36 • The Director of Technology is responsible for the management and
37 organization of all District web sites and sets parameters and
38 guidelines in conjunction with the Board and other committees.
- 39 • The Site Manager is responsible for the organization of the individual
40 web site pages, determines content and authorizes other publishing
41 efforts.
42
43

DOWNINGTOWN AREA SCHOOL DISTRICT
SCHOOL BOARD POLICY
SECTION: OPERATIONS

- District employees, Board members, or guests may not establish personal or commercial use web pages using District equipment, resources, or identification.
- Any organization dedicated to communicating information (e.g. home and school, student council, band boosters, etc.) about Downingtown Area School District should be cleared and monitored at the building level.
- All web sites are considered the property of Downingtown Area School District and therefore, are subject to monitoring.

5. **PRIVACY**

The protection of individual privacy is a concern to the Downingtown Area School District. The School District has created this privacy statement in order to demonstrate its firm commitment to privacy. The following discloses our information gathering and dissemination practices for this site.

A. **INFORMATION YOU PROVIDE TO US**

The School District does not keep any personal information about you or your visit to our Internet site unless you have specifically supplied it to us.

B. **OTHER INFORMATION ABOUT YOUR VISIT**

Like most Internet sites, our web site reads some information from your computer that helps us analyze traffic patterns, perform routine maintenance, maintain site security, and to help you navigate through our site. Generally the information we collect is temporary and deleted when you leave our system. Some of the information the School District collects and maintains is the following:

- total number of visitors to our site
- types of computer systems used to access our site
- web browser type and version
- date and time of access
- the web site you visited prior to coming to this web site
- information about possible system security threats

Occasionally the School District may have a survey on the web site that allows a visitor to vote only once. In order to keep track of whether your vote, a cookie (a simple text file) will be created and stored on your computer. This cookie is created on your computer by voting on the survey. It will not contain personally identifiable information and will not compromise your privacy or security. The only information that is contained is the name of the survey and how you voted. This cookie will remain on your computer for the duration of the survey. The cookie has an expiration date. When that date occurs it will be deleted from your computer.

DOWNINGTOWN AREA SCHOOL DISTRICT
SCHOOL BOARD POLICY
SECTION: OPERATIONS

1
2 This privacy policy does not apply to web sites operated by third parties that you may access
3 through a link from our web site.
4

5 **6. INFORMATION POSTED ABOUT STUDENTS**

6 The Web Site shall not include personally identifiable information about any student and
7 shall not include students' phone numbers, addresses, e-mail addresses, names of other
8 family members, or names of friends, except in areas that are identified as secure.
9 Information about students in grades K-12 that might reasonably be expected to be
10 published by the local media (recognition, awards, competition results, etc.) may be posted
11 and may include students' first and last names. Through secure access, authorized
12 personnel (parent, teacher, student, etc.) may view student information.
13

14 **7. INFORMATION POSTED ABOUT STAFF**

15 The full name, Downingtown Area School District mailing address, DASD telephone
16 number, DASD email address, job title and responsibilities, and professional background of
17 any DASD faculty member or staff person may be published on the DASD web site in
18 connection with the publication of (1) a general listing and profile of DASD faculty and staff,
19 (2) faculty or student work, (3) text, art photographs, graphic images, sound or other
20 material concerning school-related activities or events.
21

22 **8. USE OF PHOTOGRAPHS, VIDEOS, AND AUDIO RECORDINGS ON THE WEB**

23 Photographs, videos, or audio recordings of any student shall not be used without the prior
24 written approval of parents or guardians or students who are eighteen years of age (18) or
25 older except in areas that are identified as secure. Release of Student Information on
26 District/School Websites shall be used and must be submitted to the building office.
27

28 Photographs or videos of students in grades Kindergarten through eighth grade shall
29 contain three or more students and may not include first or last names of any of the
30 students shown with the image or in accompanying text or audio. Photographs or videos of
31 students in grades ninth through twelfth may be published without regard for whether
32 those images contain one, two, or a group of individuals. If a parent of a student has
33 specifically requested that his or her child not to be identified or included on the Web Site, a
34 request may be made in writing to the Superintendent or the Superintendent's designee and
35 such information shall be altered or removed.
36

37 Individual photographs, videos, or audio recordings of faculty and staff may appear.
38

39 **9. INFORMATION DISCLAIMER**

40 The Downingtown Area School District has made reasonably efforts to ensure the accuracy
41 of the information provided in this web site. However, due to the possibility of
42 unauthorized access to this site, data transmission errors, changes to source material made
43 since the last update to the site, or other human or mechanical errors, the information
44 contained on this web site should not be deemed reliable for legal purposes. Please contact
45 the School District Communications Specialist to verify the accuracy of the information.
46

