

DERRY TOWNSHIP SCHOOL DISTRICT

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE OF
TECHNOLOGY RESOURCES

ADOPTED: August 10, 2009

REVISED: August 27, 2012

<p>1. Purpose</p> <p>2. Authority</p> <p>47 U.S.C. Sec. 254</p> <p>P.L. 106-554 Sec. 1732</p>	<p>815.1 ACCEPTABLE USE OF TECHNOLOGY RESOURCES (Student Version)</p> <p>The Board recognizes use of the Internet and other computer networks as integral in the district's instructional and operational programs in order to facilitate learning, teaching and daily operations through interpersonal communications and access to information, research and collaboration.</p> <p>For instructional purposes, the use of network facilities shall be consistent with the curriculum adopted by the school district as well as the varied instructional needs, learning styles, abilities, and developmental levels of students.</p> <p>These guidelines and policies address the appropriate use of electronic communication tools. These tools include, but are not limited to, the following:</p> <ol style="list-style-type: none"> 1. Telephones/Cell Phones 2. Electronic mail accounts, including district e-mail and voicemail 3. Computers and network tools supplied by the district 4. Cameras (Video and Still) 5. Personal audio devices 6. Calculators <p>The electronic information available to students does not imply endorsement by the district of the content, nor does the district guarantee the accuracy of information received. The district shall not be responsible for any information that may be lost, damaged or unavailable when using the network or for any information that is retrieved via the Internet.</p> <p>The district shall not be responsible for any unauthorized charges or fees resulting from access to the Internet.</p> <p>Students must be aware that the district may, at any time, and without prior notice, access and monitor any district computer and the information contained within it. Therefore, students should expect no right to privacy pertaining to any information or files stored in, or accessed by any district computer including Internet sites and files accessed, emails sent and received, electronic folders and files, and any or all information stored or accessed on a district computer.</p>
---	---

<p>3. Delegation of Responsibility</p> <p>20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254</p>	<p>The Board establishes that network use is an essential function of learning, not a right; inappropriate, unauthorized and illegal use will result in cancellation of those privileges and appropriate disciplinary action.</p> <p>The district shall make every effort to ensure that this resource is used responsibly by students.</p> <p>Students have a responsibility to develop the intellectual skills necessary to discriminate among information sources, to identify information appropriate to their age and developmental levels, and to evaluate and use the information to meet their educational goals.</p> <p>Students have the responsibility to respect and protect the rights of every other user in the district and on the Internet.</p> <p>The administration shall have the authority to determine what is considered inappropriate use.</p> <p>The superintendent or designee shall be responsible for recommending technology and developing procedures used to determine whether the district's computers are being used for purposes prohibited by law or for accessing sexually explicit materials.</p> <p>The procedures shall include but not be limited to:</p> <ol style="list-style-type: none"> 1. Utilizing a technology protection measure that blocks or filters Internet access for minors and adults to certain visual depictions that are obscene, child pornography, harmful to minors with respect to use by minors, or determined inappropriate for use by minors by the administration. 2. Maintaining and securing a usage log of Internet usage, email, and electronic communication. 3. Monitoring online activities of users.
<p>4. Guidelines</p>	<p>Network accounts shall be used only by the authorized owner of the account for its approved purpose. All communications and information accessible via the network should be assumed to be private property and shall not be disclosed. Network users shall respect the privacy of other users on the system.</p> <p><u>Representing the District in Postings</u></p> <p>The information that students publish electronically (a "Posting") reflects on the district in general. Violation of the district's Acceptable Use Policy may damage the district reputation and could give rise to individual liabilities.</p>

<p>SC 1303.1-A Pol. 249</p>	<p><u>Limits of Privacy</u></p> <p>Email, voicemail messages and computer-stored items are district property and business records of the district and may have legal effect identical to that of traditional, hard-copy documents. They are discoverable in litigation and can be used as evidence. Accordingly, all email messages should be treated as though they may later be viewed by others.</p> <p>When stored on computers, email messages and other files typically are subject to routine backup procedures. This means that copies of these files may be retained for longer periods of time even after being deleted from a computer.</p> <p>All district emails are archived for two school years. On July 1st of each fiscal year, emails from two school years prior are deleted. For example, on July 1, 2009 (2009-2010 school-year) all emails from the July 1, 2006 through June 30, 2007 are deleted.</p> <p><u>Prohibitions</u></p> <p>Students are expected to act in a responsible, ethical and legal manner in accordance with district policy, accepted rules of network etiquette, and federal and state law. Specifically, the following uses are prohibited, yet do not constitute an exhaustive list:</p> <ol style="list-style-type: none">1. Facilitating illegal activity.2. Commercial or for-profit purposes.3. Political lobbying.4. Bullying/Cyberbullying.5. Hate mail, discriminatory remarks, and offensive or inflammatory communication.6. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.7. Access to obscene or pornographic material or child pornography.8. Inappropriate language or profanity.9. Transmission of material likely to be offensive or objectionable to recipients.
---------------------------------	--

10. Intentional obtaining or modifying of files, passwords, and data belonging to other users.
11. Impersonation of another user, anonymity, and pseudonyms.
12. Fraudulent copying, communications, or modification of materials in violation of copyright laws.
13. Loading or using of games, programs, files, or other electronic media that creates security risks, such as peer to peer file sharing software.
14. Disruption of the work of other users.
15. Destruction, modification, abuse or unauthorized access to network hardware, software and files.
16. Quoting of personal communications in a public forum without the original author's prior consent.

Security

System security is protected through the use of passwords. Failure to adequately protect or update passwords could result in unauthorized access to personal or district files. To protect the integrity of the system, the following guidelines shall be followed:

1. Students shall not reveal their passwords to another individual.
2. Users are not to use a computer that has been logged in under another student's or employee's name.
3. If the student has reason to believe that their password has been compromised, it is their duty to report the claim immediately to the administration.

Consequences For Inappropriate Use

Failure to abide by this policy may result in disciplinary action.

The network user shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts.

Illegal use of the network; intentional deletion or damage to files of data belonging to others; copyright violations; and theft of services may be reported to the appropriate legal authorities for possible prosecution.

	<p><u>References</u></p> <p>School Code – 24 P.S. Sec. 1303.1-A</p> <p>Child Internet Protection Act – 24 P.S. Sec. 4601 et seq.</p> <p>P.L. 106-554 Sec. 1732</p> <p>Enhancing Education Through Technology Act of 2001 – 20 U.S.C. Sec. 6777</p> <p>Internet Safety – 47 U.S.C. Sec. 254</p> <p>Board Policy – 249, 814</p>
--	---