3027 Use of the District's Internet and Computer Networks

The Board supports use of the Internet and other computer networks 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.

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.

The electronic information available to students and staff 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.

The District shall not be responsible for any unauthorized charges or fees resulting from access to the Internet.

The District reserves the right to log network use and to monitor fileserver space utilization by District users in order to address School District concerns. A log on banner in the form attached as Appendix A, as may be amended from time to time by the Administration, will put users on notice of the District's access right.

The Board establishes that network use is a privilege, not a right; inappropriate, unauthorized and illegal use may result in suspension and/or cancellation of those privileges and appropriate disciplinary action. The frequency and severity of violations, among other things, will determine the level of suitable discipline.

The District shall make every effort to ensure that this resource is used responsibly by students and staff, and that it complies with the Federal Communications Commission's Children's Internet Protection Act (CIPA).

This Policy 3027 and Policy 3014 (Information Systems Policy) applies to all students, employees, ECA positions, visitors and volunteers using the School District's internet service or computer network, or any School District owned device, software, application, digital technology or system whether on the school district premises or in any location away from the school district premises, including at home. In addition, this policy applies to any non school district owned device using the District's network, systems or Internet connection.

Administrators, teachers and staff have a professional responsibility to work together to help students 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.

Students and staff have the responsibility to respect and protect the rights of every other user in the District and on the Internet.

The administrators shall have the authority, in the first instance, to determine whether activity violates this policy. The determination is subject to review by the Superintendent.

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 this policy, by law or for accessing sexually explicit materials. The procedures shall include but not be limited to:

1. Utilizing a technology protection measure that blocks or filters Internet access for minors and adults to certain visual depictions that are obscene, pornographic, including child pornography, or harmful to minors with respect to use by minors.

2. Maintaining and securing a usage log.

3. Monitoring online activities on the District network or with District equipment in order to address School District concerns.

4. Educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response.

Network accounts shall be used only by the authorized owner of the account for its approved purpose. All network users shall only use their own password and shall not disclose password information to any other person.

Prohibitions

Students and staff 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.

Personal use of the District's internet and email system by staff must be strictly limited. To the extent possible, staff should not use the District's network or computers to transmit personal communications.

Specifically, the following uses are prohibited:

1. Facilitating illegal activity.

2. Commercial or for-profit purposes.

3. Nonwork or nonschool related usage.

4. Product advertisement or political lobbying.

5. Bullying/Cyberbullying.

6. Hate mail, discriminatory remarks, or offensive or inflammatory communication.

7. Communication by staff to students which do not entirely concern necessary and appropriate School District matters.

8. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.

9. Access to materials, images or photographs that are obscene, pornographic, lewd or otherwise illegal.

10. Access by students and minors to material that is determined by the District to be harmful to minors or is determined by the District inappropriate for minors in accordance with the CIPA and Board policy adopted pursuant thereto, or the student code of conduct.

11. Inappropriate language or profanity.

12. Transmission of material likely to be offensive or objectionable to recipients.

13. Intentionally obtaining or modifying of files, passwords, and data belonging to other users.

14. Impersonation of another user, anonymity, and pseudonyms.

15. Fraudulent copying, communications, or modification of materials in violation of copyright laws.

16. Loading or using of unauthorized games, programs, files, or other electronic media.

17. Disruption of the work of other users.

18. Destruction, modification, abuse or unauthorized access to network hardware, software and files.

Security

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

1. Employees and students shall not reveal their own password or the password of any other system user to any other individual.

2. Users are not to use a computer that has been logged in under another student's or employee's name.

3. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network.

Consequences For Inappropriate Use

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 will be reported to the appropriate legal authorities for possible prosecution.

General rules for behavior and communications addressed elsewhere in Board policy and the student code of conduct apply when using the Internet, in addition to the stipulations of this policy. Suspension or loss of access and other disciplinary actions shall be consequences for violations of this policy.

Vandalism will result in cancellation of access privileges and disciplinary action. Vandalism is defined as any intentional attempt to

harm or destroy data of another user, Internet or other networks; this includes but is not limited to uploading or creating computer viruses.

Copyright

The illegal use of copyrighted software by students and staff is prohibited. Any data uploaded to or downloaded from the network must be authorized by fair use guidelines or consent.

Safety

To the greatest extent possible, users of the network will be protected from harassment and unwanted or unsolicited communication. Any network user who receives threatening or unwelcome communications shall report such immediately to a teacher or administrator.

Any District computer/server utilized by students and staff shall be equipped with Internet blocking/filtering software.

Developmentally appropriate internet safety measures shall be implemented that include, but are not limited to, the following:

1. Safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications.

2. Prevention of unauthorized online access by minors, including "hacking" and other unlawful activities.

3. Unauthorized disclosure, use, and dissemination of personal information regarding minors.

4. Restriction of minors' access to materials determined by the District to be harmful to them pursuant to the CIPA and Board policy.

This Policy completely supersedes the interim Addendum adopted by the District on September 24, 2012.

ADOPTED: December 14, 2009
REVISED: November 26, 2012

APPENDIX "A"

LOG ON BANNER

The Upper St. Clair School District ("District") reserves the right to view or scan any file or software on its computers or passing through its network at any time for any purpose in order to address School District concerns. All electronic messages contain no right of privacy or confidentiality except where Pennsylvania or Federal law provides for it. The District may inspect the usage of any electronic communications made by any person at any time utilizing District hardware or passing through the District's network as deemed necessary to address School District concerns to the full extent not expressly prohibited by applicable law.

The School District's Policy 3027, Use of the District's Internet and Computer Networks, is available by clicking here.