SECTION 11 — COMPUTER/INTERNET ACCEPTABLE USE POLICY

A student's use of the District's computers and Internet resources is a privilege, not a right. Student-users of the District's computer network and Internet access are expected to use this technology as an educational resource.

Student computer network/Internet users are expected to behave responsibly in accessing and viewing information that is pertinent to the educational mission of the District. Students are required to abide by the generally accepted rules of network etiquette. These include, but are not limited to the following:

1. **Use of Appropriate Language.** The District's Internet system has been established for an educational purpose. As such, the District prohibits student users from using language which is inconsistent with an educational purpose. The use of the following type of language is prohibited:

    a. Criminal speech and speech used in the course of committing a crime (for example: threats to the President or to any other person, instructions on breaking into computer systems, child pornography, drug dealing, purchase of alcohol, gang activities, etc.);

    b. Speech that is inappropriate in the educational setting or violates District rules (such as obscene, profane, lewd, vulgar, threatening, harassing or discriminatory language or false or defamatory material about a person/organization; dangerous information that if acted upon could cause damage or present a danger of disruption; violations of privacy/revealing personal, private information about others); and

    c. In some circumstances, such as on District-sponsored student Web pages, the District may require that student publications meet a variety of standards related to adequacy of research, spelling and grammar and appropriateness of material (i.e., that school Web pages must relate to school and career preparation activities).

2. Sending, receiving, transferring, viewing, sharing or downloading obscene, pornographic, lewd or otherwise illegal materials, images, videos or photographs, including but not limited to sexually explicit images or images portraying nudity.

2. **Access to Information.** Students are prohibited from accessing the following categories of material or information on the Internet or World Wide Web:

    a. material that is profane or obscene;

    b. material that is pornographic, expressly including child pornography;

    c. material that is harmful to minors (i.e., pictures or visual depictions which, taken as a whole, appeal to a prurient interest in nudity, sex or perverted or lewd acts);

    d. material that advocates or condones the commission of unlawful acts; or

    e. material that advocates or condones violence or discrimination towards other people.

    Students are advised that the District utilizes a Technology Protection Measure that blocks or filters Internet access to the above categories of material/information, as well as other categories of material or information which the District has deemed inappropriate for viewing by students in the educational setting.

4. Online Safety/Privacy: Students are required to complete an Internet safety course. The curriculum will focus on educating students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response. The course content will be prescribed to the building principals by a designated administrator within the

District's IT Department at the beginning of each school year. The IT administrator will ensure the content is consistent with federal requirements.

Students are prohibited from giving out personal information for non-educational reasons pertaining to themselves such as: addresses, telephone numbers, parents' work addresses or telephone numbers or the name and location of their school, even through email correspondence unless specifically authorized by the District and with the consent of the students' parents/guardians. Students must tell their teachers and/or parents immediately if they come across information which makes them feel uncomfortable. Students must never agree to get together with someone they "meet" online without first discussing it with their parents. If their parents agree to the meeting, students must ensure that the meeting is in a public place and that they are accompanied by one of their parents.

Only Web 2.0/Social Networking tools and applications, including but not limited to instant messaging, chat rooms, wiki spaces, blogs and other methods of interactive electronic communication, approved by a designated administrator within the IT Department, and aligned to the National Educational Technology Standards for Students (NETS*S) may be utilized for instructional purposes in the attainment of the educational goals of the District. Technology Protection Measures are in place to block or filter Internet access to non-approved Web 2.0 tools and applications. Any digital communications are subject to District review at any time. Technology Protection Measures will be used to red-flag digital communications that violate Pennsylvania or federal law or District policy. Routine maintenance and monitoring of the District's system may lead to discovery that a student has violated the law or a District policy. An individualized search of a student's profile, log files, history, etc., will be conducted if there is reasonable suspicion that a user has violated the law or District policy.

5. Electronic Mail (email): Students may only use email solutions approved by a designated administrator within the IT Department. Students must understand that there is no guarantee of privacy in their email messages and that email messages are subject to District review at any time. Technology Protection Measures will be used to red-flag emails that violate the law or a District policy/rule. Routine maintenance and monitoring of the District's system may lead to discovery that the student has violated the law or a District policy/rule. An individualized search of a student's email will be conducted if there is a reasonable suspicion that a user has violated the law or District policy/rule. Email should be used only for legitimate educational purposes or as authorized by the District. Students should be courteous and respectful in their email messages to others. The use of students' email accounts will be permitted for instructional purposes aligned to the National Educational Technology Standards for Students (NETS*S) and for the attainment of the District's educational goals.

6. Plagiarism: Students are reminded that it is plagiarism to "cut/copy and paste" information from the Internet and then pass it off as their own original ideas. Students are prohibited from plagiarizing information and resources from the Internet and are reminded to cite proper sources used from the Internet.

7. Copyright Infringement: All communications and information via the network (i.e., the Internet) should be assumed to be private property and protected by copyright. Students may not reproduce copyrighted material without explicit permission of the author/owner. Only public domain software can be downloaded.

8. Unauthorized or Disruptive Use/Hacking: Students are prohibited from using the District network in such a way that would disrupt the use of the network by other users. Students may not create or maliciously distribute computer viruses. Students may not destroy another person's data. Students may not access or attempt to access other computer systems or access files without authorization.

9. Purchase of Products or Services: Students are prohibited from purchasing products or services through the District network. The District is not responsible for any financial obligations arising from unauthorized use of the District network for the purchase of products or services.

10. Student Passwords/Accounts: Students may not share their passwords to anyone nor allow unauthorized network access via their account.

11. Unauthorized Disclosure, Use or Dissemination of Personal Information: Students may not disclose, use or disseminate personal information about students, especially minor students, without the authorization of that student's parent/guardian and without specific authorization from the District.

12. Prohibition on Using Peer-to-Peer Networking Applications: Students are prohibited from using peer-to-peer networking applications on the Internet/World Wide Web.

13. Personal Electronic Communication Devices: Students are permitted to bring their personal electronic communication devices to school and onto the District's network as set forth in the District's Electronic Devices Policy. Personal electronic devices are permitted only on the District's SDCE Wireless network. District users, both students and staff, must use their District computer login credentials in order to connect to the SDCE wireless network. The District's Computer/Internet Acceptable Use Policy and all other District policies apply to the use of personal electronic communication devices. Reconfiguration of device settings may be required to access the District's network.