APPROPRIATE USE OF TECHNOLOGY RESOURCES AND INTERNET SAFETY RESPONSIBLE USE BY STUDENTS

Student access to the internet in the District as an educational resource is automatic unless a parent or guardian notifies the school in writing as required by Board Policy IMBB, Exemptions from Required Instruction. User accounts are to be used mainly for identified educational purposes. Limited personal use is permitted if the use imposes no tangible cost on the District, does not unduly burden the District's computer or network resources, and has no adverse effect on a student's academic performance. Users will be held responsible at all times for the proper use of accounts.

The District adopts the approach of helping students become responsible users of digital media. All users of D11 computers and networks are expected to abide by the generally accepted rules of network etiquette (netiquette) and adhere to the following provisions listed below. Inappropriate use includes:

1. Disabling or attempting to disable or circumvent any internet filtering device that restricts access to harmful material.

2. Borrowing someone's account or accessing another individual's materials without authorized permission, including hacking and other unlawful activities.

3. Unauthorized disclosure, use, and dissemination of personal information including posting personal information such as addresses and phone numbers.

4. Vandalizing, damaging, or disabling the system by physical force or by introducing any computer code designed to hinder the performance of a computer's memory, file system, or software.

5. Downloading or using copyrighted information without permission from the copyright holder (including installation of unlicensed software).

6. Posting, sending, accessing, or displaying electronic mail, chat rooms and other forms of direct electronic communication that are abusive, obscene, sexually oriented, threatening, harassing, cyber bullying, or illegal.

7. Wasting school resources through the improper use of the computer system, such as downloading, distributing, or executing files not specifically related to classroom assignments.

8. Gaining or attempting to gain unauthorized access to restricted information or resources.

9. Tampering with equipment except as directed by the person in charge.

10. Removing equipment from the site without written permission from a teacher or administrator.

11. Unauthorized wireless network technologies may NOT be installed or utilized while on District property.

I agree to abide by the provisions listed above and understand that consequences for inappropriate use include suspension of access to the system and revocation of the computer system account and/or other disciplinary or legal action in accordance with the Student Conduct, Discipline and Attendance Handbook and applicable laws.

Revised April 27, 2016