Irvington Community Schools, Inc.
Student Acceptable Use Policy – Long Form
Guidelines and Contract for School Computers and Internet

The use of school computers and Internet is a privilege, not a right. Students using school computers and ICS's Internet must do so responsibly and appropriately. The user is personally responsible for his/her actions is accessing and utilizing the school's computer resources. Failure to comply with the policies and guidelines set forth may result in the loss of computer and/or Internet use at school or other disciplinary or legal action taken by the school and any involved parties.

School computers should be used as an educational tool. The use of computers and Internet at school must always be approved by a teacher and under staff supervision. Computers should be used for educational programs and activities or teacher assignments that require research, word processing, presentation, etc. Use of school computers and Internet for entertainment purposes, such as playing games and accessing non-educational websites, should be limited to incentives or rewards from teachers.

Use of personal devices—including laptops, netbooks, tablets, MP3 players/iPods, cell/smart phones—is not permitted during the school day. These items will be confiscated and turned over to the Behavior Coach if discovered in the hallways or classrooms. Graphing calculators are allowed. ICS is not responsible for the loss or damage of personal devices that are brought onto school property.

Inappropriate Use – The following activities are considered violations of the intended use of school computers and/or the network:

1. Accessing the control panel and/or changing any settings on school computers, including changing the desktop background, renaming icons, modifying the screen saver, etc.
2. The alteration of Internet browser settings, including changing the history settings and clearing the history, cache, cookies, etc.
3. Downloading and installing commercial software, shareware, or freeware to a computer's hard drive or a network (shared) drive, including applications and games from Internet websites.
4. Accessing personal E-mail from school computers without permission from a teacher, and/or using E-mail for communicating with friends or family during the school day. The use of personal E-mail at school is limited to transferring assignments to a teacher or for home access.
5. Using school computers for personal business, entertainment, or social communication (e.g., instant messaging, message boards, chat rooms, social networking, etc.) not relating to school activities.
6. Attempting to access blocked websites and/or trying to bypass the web filter.
7. Using headphones for entertainment media (e.g., music, music videos, movies, etc.) unless media has been approved by a teacher. Likewise, external devices such as MP3 players should not be connected to school computers. USB flash drives are permitted.
8. Damaging school computers or hardware, including LCD monitor screens. Food, drinks, candy, and gum are prohibited from the computer lab and computer workstations throughout the school.
9. Disconnecting computer peripherals, including the monitor, mouse, keyboard, headphones, etc.
10. Misuse or overuse of technology resources, such as storage space, bandwidth, and printing consumables (i.e., paper and ink). Only save files, graphics, etc. necessary for school assignments and delete files that are no longer needed. Do not print unless given permission by a teacher.

Unethical Use – The following activities are considered violations of social standards of conduct:

1. Using profane, abusive, or impolite language when communicating over the Internet. Any threats, (cyber)bullying, harassment, racial slurs, etc. made via electronic communication will be taken seriously and may include law enforcement intervention.
2. Accessing websites that contain inappropriate content. Accessed websites should not contain adult content or profanity and should not advocate illegal activities, violence, or discrimination.
3. Disclosing personal information, contact information, or account information (i.e., user names and passwords) for yourself or any other person.
4. Posting the school's name or defamatory or threatening remarks against the school, faculty, or other students online.
5. Using the school's network for commercial gain or profit. This includes entering online contests, accessing online auction websites (e.g., eBay), and online gambling. Likewise, using the school's network to make online purchases is not allowed.

Illegal Use – The following activities are violations of local, state, and/or federal laws:

1. Violating anti-piracy laws by the unauthorized reproduction and/or distribution of copyrighted materials (e.g., music, movies, art, photography, and software). This includes burning copies of CDs, DVDs, and software. Criminal copyright infringement, including infringement without monetary gain, is subject to investigation by the FBI and punishable by confinement and fines.
2. Plagiarizing works published on the Internet. Plagiarism is taking someone else's writing or ideas and claiming them as your own. Likewise, you should not claim media you did not create as your own. Sources should always be cited, giving credit to the owner or creator.
3. Accessing or attempting to access another user's account(s). Altering or deleting files belonging to another user and the forging of E-mail are prohibited. Unauthorized access to another user's accounts, folders, and files is considered hacking.
4. Making deliberate attempts to disrupt computer systems, the network, or destroy data by the spreading of computer viruses or by writing and executing damaging code.
5. Engaging in Internet fraud.
6. Creating, possessing, and/or distributing child and/or adult pornography.
7. Theft or vandalism of computers and related equipment, including classroom technology.

Potential Consequences for Violations of the Acceptable Use Policy:

1. Suspension or revocation of computer access.
2. Suspension or revocation of Internet access.
3. Liability for expenses incurred due to misuse, theft, vandalism, or deliberate damage to computer systems and/or the network.
4. School suspension or expulsion.
5. Legal action and prosecution by the authorities.

Note: Network administrators have the right to monitor all activity on the school network. Additional guidelines and restrictions may be added at any time, as determined by school leadership.

Please sign and date the attached <u>short form</u> of the Student Acceptable Use Policy and return only that page to the school. You may retain this long form for your records and reference.