aspen | PUBLIC SCHOOLS

Internet and Device Acceptable Use policy (Students/Parents)

A. INTRODUCTION

Welcome to the document that sets out our electronic policy!

Although it is a long and detailed policy, it is very important that you read it thoroughly because it explains everything you need to know about using the Internet, computers and other devices at a Aspen Public schools. It is your responsibility to use the Internet in ways that follow and support this policy.

If you know the behaviors and limits set out in this policy, you will become a successful electronic user at school. All electronic usage throughout the Aspen schools, including the things you do on a day to day basis, will be governed by this policy document. Your use - or misuse - of any electronics while at school will be interpreted according to this policy.

If you have any questions about the expectations set out in this document, please contact the Site Director of your school site.

B. GENERAL PRINCIPLES OF ACCESS

Aspen Public Schools provides access to the Internet, including access to email, for its schools, faculties, students, and guests. (Guests include, but are not limited to, parents, student teachers, temporary employees, parent volunteers, and other school volunteers). All Internet access, including the use of email, occurs through the use of the APS's system.

This Internet and Device Acceptable Use Policy governs all electronic activity, including email and access to the Internet, which is undertaken by APS faculties, students, and parents/guardians either in their official APS capacity or as part of the educational, instructional or extracurricular programs connected to the APS. No APS faculty member, student, guest or parent/guardian may engage in activities prohibited by this policy, whether through the APS's Internet service or through any other Internet Service Provider, for whatever reason. Parents are strongly encouraged to discuss and monitor their child's school Internet use and to discuss any issues or concerns that they may have with the school's teacher and administrators. All use of the Internet will be governed by this policy.

B. TECHNOLOGY TEAM RESPONSIBILITIES

1) The Chief Technology Officer, or his/her designee, will serve as the coordinator to oversee Internet access via use of APS systems.

2) The Executive Director and Site Directors of each school are responsible for the dissemination of this Internet and Device Acceptable Use Policy, and they will work to enforce this policy on their site.

3) APS reserves the right to revise this Internet and Device Acceptable Use Policy, as it deems necessary, and it will always post the current policy on each of the school's websites as notice to users of any revisions.

C. LIMITATION OF LIABILITY

1) APS makes no warranties of any kind, either express or implied, that the functions or the services provided by or through the APS system will be error-free or without defect. APS will not be responsible for any damage users may suffer, including but not limited to, loss of data or interruptions of service. APS is not responsible for the accuracy or

quality of the information obtained through or stored on the system. APS will not be responsible for financial obligations arising from a user's unauthorized use of the system.
2) Users will indemnify and hold APS and its respective schools harmless from any losses sustained by APS as a result of intentional misuse of the system by user.

D. FILTERING

APS has installed Internet filtering software in an attempt to block user access to inappropriate and/or harmful content on the Internet. Filtering technology is not perfect, and therefore, may in effect interfere with legitimate educational research. No filtering software is one hundred percent effective and occasionally fails. In the event that the filtering software is unsuccessful and children gain access to inappropriate and/or harmful material, APS and individual school sites will not be liable.

Families may wish to see how the APS filter system guidelines adhere to the US Congress enacted CIPA guidelines, with rules updated to 2011: http://www.fcc.gov/guides/childrens-internet-protection-act

The filter is set at the most restrictive setting in restricting access to Internet sites that may contain interactive chat or mail or information regarding:

- Sex acts
- Sex attire
- Sex/nudity
- Sex/personal
- Basic sex education
- Advanced sex education
- Sexuality
- Sports
- Gambling
- Pornography
- Hacking
- Proxy avoidance
- Addictions
- Forums
- Social Networks
- Violence
- Streaming Music
- Non Academic Videos
- Illegal Drugs
- Weapons
- Criminal Activity
- Chat
- Hate and Intolerance

E. REGULATIONS OF ACCESS

1) Important Consequences of Access

a) APS will always cooperate fully with local, state, or federal officials in any lawful investigation concerning or relating to any illegal activities conducted through the APS system.

b) Internet access is a privilege, not a right, and all students should be aware that APS may revoke Internet access for any reason. If a student's access is revoked, APS will provide an explanation for the revocation, and the school site will ensure that the student continues to have equal access to participate in the educational program.

c) It is very important for students and families understand that violations of this Internet and Device Acceptable Use Policy DO count as disciplinary actions. All violations of this policy will be addressed according to the Restorative Discipline plan of the school that the student attends. Students and their families WILL have to meet specific concerns related to the violation and cooperate with the school to help the student acquires the specific behaviors necessary to behave appropriately on an electronic network.

2) Privacy: It is important that all users of the APS system understand that there is no expectation of privacy on this system.

a) APS reserves the right to monitor the use of the Internet through its system at all times. APS will collect and store information about usage which includes, but may not be limited to, the date and time a user visits the site and information about the user's activities while online. Any information gathered is obtained solely for the purpose of improving APS services and providing the system with statistical information to assist in improving teaching and learning by teachers and students respectively. Except as otherwise provided in this Internet and Device Acceptable Use Policy, APS will not use cookies to gather personal identifying information about any of its users. (Cookies are computer programs that allow APS, among other things, to verify whether a visitor is an authorized user of the APS system and then store information about a user on a computer hard drive or disk.) Personal identifying information includes, but is not limited to, names, home addresses, email addresses and telephone numbers.

b) As required by the Children's Internet Protection Act ("CIPA"), APS will monitor students' online activities. Such monitoring may lead to discovery that the user has violated or may be violating, APS Internet and Device Acceptable

Use Policy, the student handbook, or the law. APS also reserves the right to monitor other users (e.g., non students) online activities.

c) APS reserves the right to employ and review the results of software that searches, monitors and/or identifies potential violations of the Internet and Computer Acceptable Use Policy.

d) Users should be aware that their personal files may be discoverable in court and administrative proceedings and in accordance with public records laws.

e) System users should have no privacy expectation in the contents of their personal files and records of their online activity while on the APS system. APS does not encourage users to store personal data on the APS system - APS cannot be responsible for the loss or damage of such data.

3) Parental Notification and Responsibility

a) Where appropriate, individual schools will provide students and parents with guidelines and instructions for student safety while using the Internet.

b) APS Internet and Device Acceptable Use Policy contains restrictions on accessing inappropriate material. However, there is a wide range of material available on the Internet, some of which may or may not fit the particular values of the students. While student use will be supervised and logged, it is not practically possible for APS to monitor and enforce a wide range of social values in student use of the Internet. Further, APS recognizes that parents bear primary responsibility for transmitting their particular set of family values to their children. APS strongly encourages parents to specify to their child(ren) what material is and is not acceptable for their child(ren) to access through APS system.

4) Access

a) Students will generally be provided with Internet access. This document describes the terms of that access. In addition, a school may decide to create a written agreement or “compact” with parents that expands the terms and responsibilities of the student, parent and school in further detail. However, that written agreement may not permit any Internet or email activity prohibited by this Internet and Device Acceptable Use Policy, and it may not prohibit any such activity permitted by this Policy.

5) Limitations on Internet Usage

A) Personal Safety Violations For Students

APS strongly recommends that all students follow the two guidelines below, at all times: i) students do not post or transmit photographs or personal contact information about themselves or other people. ii) Students do not agree to meet with someone they have met online.

APS does require that student users promptly disclose to their mentor or other school employee any electronic message they receive that is inappropriate or makes them feel uncomfortable.

B) Illegal Activities: All students need to be aware that engaging in any of the following illegal activities will result in disciplinary action by their school.

1) Users shall not attempt to gain unauthorized access to the APS system or to any other computer system through the APS system or go beyond their authorized access. This prohibition includes intentionally seeking information about passwords belonging to other users, modifying passwords belonging to other users, illegally obtaining wireless passkeys, or attempting to log-in through another person's account. Further, users may not attempt to access, copy, or modify another user’s files. These actions are not permitted and may be illegal, even if only for the purposes of "browsing.”

2) Users shall not attempt to subvert network security, impair the functionality of the network or bypass restrictions set by network administrators. Users are also prohibited from destroying data by spreading computer viruses or vandalizing data, software or equipment.

3) Users shall not use the APS system to engage in any other illegal act, such as arranging for a drug sale, engaging in criminal gang activity, threatening the safety of a person, etc.

4) Users shall not use the APS system to download illegal music, books, video, and software without payment to the originator.

5) User shall not use software applications that have a continuous connection to the internet that is streaming steadily

and consuming large amount of internet bandwidth (e.g. bit-torrent, etc) for the purpose of obtaining illegal content.

C) System Security Violations

1) Users are responsible for the use of their individual account if applicable and should take all reasonable precautions to prevent others from being able to use their account. Under no conditions should a user provide their password to another person, except that mentors and/or teachers may require users to provide their passwords.

2) Student users will immediately notify a teacher if they identify a possible security problem (such as disclosure of their password to another person) and other users will immediately notify the Technology Team. No users will go looking for security problems because this may be construed as an illegal attempt to gain access.

[APS will install and maintain anti-virus software on each computer as required. Updates, typically referred to as "virus definitions," will be updated as the manufacturer recommends.]

D) Inappropriate Language

All students should be aware that using inappropriate language electronically can be damaging to others and may lead to disciplinary action.

1) Restrictions against inappropriate language apply to public messages, private messages, and material posted on Web pages.

2) Users will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, abusive or disrespectful language.

3) Users will not post information that could interfere with the educational process or cause a danger of disruption in the educational environment.

4) Users will not engage in personal attacks, including prejudicial or discriminatory attacks.

5) Users will not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a user is told by a person to stop sending them messages, they must stop.

6) Users will not knowingly or recklessly post false or defamatory information about a person or organization.

7) Users should not repost a message that was sent to them privately without permission of the person who sent them the message.

8) Users should not post private information about another person.

E) Respecting Resource Limits

1) Users will use the system only for educational and professional activities.

2) Users will not download large files unless absolutely necessary. If necessary, users will download the file at a time when the system is not being heavily used.

3) Users will not post chain letters or engage in "spamming." Spamming is sending an annoying or unsolicited message to many people, except that an unsolicited message sent by a supervisor, relating to work activity does not constitute spamming.

4) Users will check their email frequently and delete unwanted messages.

5) Users will not send email containing commercial links unless the link is predominantly instructional in nature.

F) Plagiarism and Copyright Infringement

1) Users will not plagiarize works that they find on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were original to the user.

2) Users will respect the rights of copyright owners and not infringe on those rights. Copyright infringement occurs when an individual inappropriately reproduces a work that is protected by a copyright. If a work contains language that specifies acceptable use of that work, the user should follow the expressed requirements. If the user is unsure whether or not they can use a work, they should request permission from the copyright owner.

G) Access to Inappropriate Material

1) Users will not use the APS system to access material that is profane or obscene (e.g., pornography), that advocates illegal or dangerous acts, or that advocates violence or discrimination towards other people (e.g., hate literature). For students, a special exception may be made if the purpose is to conduct research and is approved by the teacher.

2) If users inadvertently access such information, they should immediately disclose the inadvertent access in a manner specified by their school. This will protect users against an allegation that they have intentionally violated the Internet and Device Acceptable Use Policy.

H) Other

1) Users will not use the Internet for advertising, promotion, commercial purposes or similar objectives.

2) Users will not use the Internet to conduct for-profit business activities or to engage in religious activities. Users are also prohibited from engaging in any non-governmental-related fund raising or public relations activities such as solicitation for religious purposes, lobbying for political purposes, or soliciting votes. APS is not responsible for this or any other commercial activity users engage in.

F) Email Policy:

Email resources are available to all Aspen users. Every individual assigned a Aspen email address will have the responsibility to use this resource in an efficient, effective, ethical and lawful manner. The following actions are prohibited:

A) Email Acceptable Use Guidelines

“Acceptable” email activities are those that conform to the purpose, goals, and mission of APS and to each user's job duties and responsibilities. Users shall have no right to privacy while using APS internet or email system. email may not be used for personal purposes during working hours, except that users may engage in minimal email activities for personal purposes, such as family correspondence, if the use does not diminish the student's productivity, work product, or ability to perform services for APS.

“Unacceptable” use is defined generally as activities using APS hardware, software, or networks at any time that does not conform to the purpose, goals, and mission of APS and to each user's job duties and responsibilities. The following list, although not inclusive, provides some examples of unacceptable uses:

1. Opening unknown email attachments or introducing computer worms or viruses. Users are prohibited from performing any activity that will or may cause the loss or corruption of data or the abnormal use of computing resources (degradation of system/network performance).

2. Using email services for private commercial or business transactions and any activity meant to foster personal gain.

3. Conducting non-APS fund raising or public relations activities such as solicitation for religious and political causes or not-for-profit activities.

4. Transmitting threatening, offensive harassing information (messages or images) containing defamatory, abusive, obscene, pornographic, sexually oriented, racially offensive, or otherwise biased, discriminatory, or illegal material.

5. Attempting to subvert network security, impair functionality of the network, or bypass restrictions set by the network administrators. Assisting others in violating these rules by sharing information or passwords.

6. Distributing "junk" mail, such as chain letters, advertisements, or unauthorized solicitations.

REMINDER: APS reserves the right to examine any/all email or Internet correspondence for security and/or network management purposes. Violation of this email policy may result in disciplinary action.

G) Device Use:

The device resources of APS are available to authorized students and parents for educational, research, and administrative purposes. In order to maintain this policy, it is essential that the users themselves observe reasonable standards of behavior regarding the use of the devices. The following actions are prohibited:

- Any attempt to modify or damage device equipment, including marking the device in any way, placing stickers or writing on the device
- Any attempt to modify or damage device, network, or software
- Any attempt to modify the original system configurations
- Improper use of the device equipment
- Installation of non-academic games on APS systems
- Recreational game playing
- Unauthorized use of an APS account belonging to another user
- Unauthorized reading, use of, or deletion of private files or email belonging to another user
- Sharing username and passwords with other users or any other person
- Any attempt to circumvent (hacking/bypass) system protection and security features
- Knowingly using any system to produce system failure or degrade performance
- Engaging in unauthorized duplication, alteration or destruction of data, programs or software
- Transmitting or disclosing data, programs or software belonging to others or duplicating copyrighted materials
- Use of device resources for private purposes, including, but not limited to, the use of device resources for profit making or illegal purposes

APS reserves the right to investigate any of the above abuses, as well as any other interference with the proper functioning of the APS network or infringements upon another user's rights. Any violation will result in disciplinary action. Consequences may include requiring students to support with tech repairs and upkeep (in alignment with restorative justice principles) or loss of device use for a short or extended period of time. If the abuse of the devices is severe, it may include the family's repaying schools for the cost of replacing the device.

H) Cyberbullying:

Bullying through the use of technology or any electronic communication, including, but not limited to, a transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted by the use of any electronic device, including, but not limited to, a computer, telephone, cellular telephone, text messaging device and personal digital assistant is prohibited. California anti-bullying laws is enforced by the following: California Education Code 32261-32262, 32265, 32270, 35294.2, and 48900

These actions are prohibited:

- Flaming
- Denigration also known as "dissing”
- Bash boards
- Impersonation
- Outing
- Trickery
- Exclusion
- Harassment
- Happy slapping
- Text wars or attacks
- Negative Online polls
- Sending malicious codes
- Griefing

Users should always use netiquette (network etiquette) when posting or replying on the internet. Always be kind, have common courtesy, and be considerate to others. Displaying online social behaviors that model good cyber citizenship is emphasized and encouraged.

aspen | PUBLIC SCHOOLS

Internet and Device Acceptable Use policy (Students/Parents)

ACKNOWLEDGEMENT OF INTERNET AND DEVICE USAGE POLICY.

Please sign and return just this page to the homeroom teacher and keep the policy document for your review.

Student Name:____Date___________________

Homeroom teacher:____

Parent Signature:____