

Washington District 50 Schools
STUDENT AUTHORIZED USE AND INTERNET SAFETY POLICY (AUP)

In accordance with: [Children's Internet Protection Act \[CIPA\]](#) / [Children's Online Privacy Protection Act \[COPPA\]](#)

Washington District 50 Schools provides all students' access to the Internet, network resources, as well as, devices at designated graded levels, as a means to promote achievement and provide diverse opportunities during the educational experience. This policy provides guidelines and information about the limitations that the school imposes on use of these resources. In addition to this policy, the use of devices, such as, but not limited to: computers, iPads, iPods, or Chromebooks, require students to abide by the Washington District 50 Schools Technology Use Guidelines, as stated in the District 50 Student Code of Conduct. This agreement comes with understanding that students will assume responsibility in the use and care of the device. Additional rules may be added as necessary and will become a part of this policy.

Washington District 50 Schools currently offers tools such as Google Apps for Education to its students. GAFE is a free service to the school and provides: document, spreadsheet, presentation, forms, & website creation. Our Google Apps account offers a calendar and email, in addition to many free educational apps. Email accounts are assigned to 6th-8th grade students, can only be used in district and do not allow sending or receiving emails from users outside our Google Apps domain. This helps secure your child from unwanted mail like solicitations & marketing. Google Apps for Education allows 21st century learners to share documents & collaborate with staff and peers from any device with internet access.

TERMS OF THE AUTHORIZED USE AND INTERNET SAFETY POLICY

Specifically, the student will adhere to these guidelines each time the Internet is used at school.

COPYRIGHT

1. Will follow copyright laws and should only download files to district owned technology that he/she is authorized or legally permitted to reproduce, or for which he/she has the copyright.

PERSONAL INFORMATION

1. Will never reveal identifying information, files, or communications to others through email or post to the Internet.
2. Do not reveal personal addresses or phone numbers.
3. Will not share passwords or attempt to discover passwords. Sharing a password could make you liable if problems arise with its use and subject to disciplinary action.
4. Do not use another user's password to access the network or internet.
5. Do not trespass into another user's files.

COMMUNICATION

1. Will use appropriate language in all communications avoiding profanity, obscenity, and offensive or inflammatory speech. Digital citizenship should be followed conducting oneself in a responsible, ethical, and polite manner.
2. Cyber bullying such as personal attacks and/or threats on/against anyone made while using district owned technology are to be reported to responsible school personnel.
3. Email may be provided for 6th - 8th grade students to use in a school related capacity. This account will be filtered and monitored, and students are to have no expectation of privacy regarding information they email.

NETWORK

1. Will not attempt to override, bypass, or otherwise change the Internet filtering software or other network configurations.
2. Changing or removing operating systems or applications is prohibited.
3. Altering or attempting to bypass security software is not allowed.
4. Will not attempt access to networks and other technologies beyond the point of authorized access. This includes attempts to use another person's account and/or password.
5. Will not connect any personal technologies such as storage devices, computers, phones, tablets, wireless access points and routers, printers, etc to district owned and maintained local, wide, or metro area network.

UNACCEPTABLE DEVICE USE

1. Loaning your device or using someone else's device, charger, or cords.
2. Leaving your device unattended inside, outside, or near a water source.
3. Having or consuming food or drinks near the device.
4. Placing the device near the edges of furniture, on floor, or in a sitting area such as couches or chairs.
5. Stacking objects on top of your device or in a locker.
6. Defacing a device with stickers, markers, graffiti, or removing any tags placed there by the tech staff.
7. Damaging devices, networks, or engaging in acts of vandalism. Vandalism is defined as the intentional attempt to harm or destroy the equipment and/or data. This includes, but is not limited to, the uploading or creation of device viruses. Vandalism is a major infraction of the rules and may result in police notification.

CLASSROOM EXPECTATIONS

1. Always properly handle the device and place securely on a working flat surface at all times.
2. Students should use the device for tasks deemed appropriate by the teacher.
3. Device is used in accordance to the assignment or verbal instructions of the teacher.
4. Will use technology for school-related purposes only during instructional time.
5. Remain in blackout mode (closed lid or device is in sleep mode) until device is required.
6. Before any free time on your device is given in class, including study hall, all missing or incomplete work must be acceptably completed.
7. Printing of materials is permitted only in the technology lab and only with specific permission. Only what is

needed for the assignment should be printed if permission is given.

8. Do not send out bulk e-mail, including chain letters, ads, or any other message that includes multiple recipients without their consent. Students must receive prior approval before any e-mail is sent to an entire class.
9. Downloading of any file should be done only with permission of a teacher and be used only for educational purposes. Programs, Apps, extensions or plugins should never be downloaded and/or installed to a device by a student.
10. The device volume should be muted when using it in a setting that would be distracting to others. Students are required to bring earbuds or headphones to class daily.
11. Students are responsible for keeping and backing up any files needed for school work to their provided Google Drive. The school is not responsible for and loss of files kept locally on a device.
12. Devices must be stored in teacher designated docking stations when not in use.
13. Devices taken to lunch or the gym should be kept in a safe area.
14. During athletic or special after-school events, devices should be stored in secure locations provided by the school. Understand that access to those sites may be restricted until the function is over.

INSPECTIONS

1. Internet browsing history must be kept intact and should not be erased by the students. Students will make available for inspection by a school official, upon request, any messages or files sent or received. Students can have no expectation of privacy and can expect teachers or administration to conduct spot checks of their Internet history, documents, email, etc.
2. Students will not make use of materials or attempt to locate materials that are unacceptable in a school setting. This includes, but is not limited to pornographic, obscene, graphically violent, racist or vulgar images, sounds, music, language, video, or other materials. All district owned technologies should be free at all times of any inappropriate material.
3. Through the use of firewall and content filtering systems, District 50 monitors device and Internet usage and attempts to block access to inappropriate and/or obscene material as best it can. Attempts to access inappropriate material will be logged and referred for disciplinary action. Accidental access to inappropriate material should be reported to school staff immediately so staff are able to ensure future access to the material is blocked. Failure to report accidental access of material may result in disciplinary action.

CONSEQUENCES

Refusal to follow these expectations may result in consequences ranging from the following- warning, limited access, denial of privileges, detention, Saturday School, OSS, possible expulsion, and notification to the authorities. School staff reserve the right to determine appropriate consequences.

PARENT & GUARDIAN EXPECTATIONS

Parents are asked to support 21st Century learning by promoting responsibility for the device and digital citizenship at home through the review of expectations laid out in this agreement. If you would like more information regarding digital citizenship, please contact your child's teacher.

By signing this you agree to abide by the conditions listed above and assume responsibility for the care and proper use of Washington District 50 Schools technology, including personally backing up personal data. Washington District 50 Schools is not responsible for any loss resulting from delays, non-deliveries, missed deliveries, lost data, or service interruptions caused by user errors, omissions or reasons beyond the district's control.

Information obtained via the Internet and other sources using Washington District 50 Schools technologies is not guaranteed as to its accuracy or quality. I understand that should I fail to honor all the terms of this Policy, future Internet and other electronic media accessibility may be denied. Furthermore, I may be subject to disciplinary action outlined in the Washington District 50 Schools Student Code of Conduct and, if applicable, my device or computer may be recalled.

I understand that access is designed for educational purposes and that the District has taken precautions to eliminate controversial material. However, I also recognize it is impossible for the District to restrict access to all controversial and inappropriate materials. I will hold harmless the District, its employees, agents, or Board Members, for any harm caused by materials or software obtained via the network.

I have discussed the terms of this Authorization with my child. I am aware that due to COPPA regulations as stated in this document, that if my child is under 13 years of age, it is necessary to give permission for my child to access various educationally related sites & Web 2.0 tools.

Herein, I am giving consent for my child to be allowed access to the District's devices, WEB 2.0 tools, & Internet. By signing below, I give permission for the school to allow my son or daughter to have access to the Internet under the conditions set forth above.

Parent/Guardian (please print): _____

Parent/Guardian Signature: _____ Date: _____

As the student, my signature indicates I have read or had explained to me and understand this Authorized Use Policy, and accept responsibility for abiding by the terms and conditions outlined and using these resources for educational purposes.

Student (please print): _____

Student Signature: _____ Date: _____

Terms and Conditions: This AUP is valid through June 30, 2018