WCSD Acceptable Use Policy

PURPOSE: Walton County School District provides all students and staff access to the Internet, network resources, and computing 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 the school imposes on using these resources.
In addition to this policy, students must abide by the WCSD Technology Use Guidelines as stated in the Student Code of Conduct when using any school computing device. Additional rules may be added as necessary and will become part of this policy.

This list of guidelines aims to ensure that all persons who use WCSD technology resources, both students and employees, use these valuable resources appropriately.

TERMS OF THE REQUIRED USE AND INTERNET SAFETY POLICY
Specifically, the student:

- Will adhere to these guidelines each time the Internet is used at home and school.
- Will make available for inspection by an administrator or teacher upon request any messages or files sent or received at any Internet location. Files stored and information accessed, downloaded, or transferred on district-owned technology are not private.
- Will use appropriate language in all communications, avoiding profanity, obscenity, and offensive or inflammatory speech.
- Understand that Cyberbullying, such as personal attacks and/or threats on/against anyone made while using district-owned technology to access the Internet or local school networks, should be reported to responsible school personnel. Rules of netiquette should be followed to conduct oneself in a responsible, ethical, and polite manner.
- Will follow copyright laws and should only download/import music or other files to a district-owned technology that he/she is authorized or legally permitted to reproduce or for which he/she has the copyright.
- Will never reveal identifying information, files, or communications to others through email or post to the Internet.
- Will not attempt to access networks and other technologies beyond the point of authorized access. This includes attempts to use another person's account and/or password.
- Will not share passwords or attempt to discover passwords. Sharing a password could make you liable if problems arise with its use and subject you to disciplinary action.
- Will not tamper with computer hardware or software, attempt unauthorized entry into computers, or vandalize or destroy computing devices or computer files. Damage to computing devices may result in felony criminal charges.
- Will not attempt to override, bypass, or otherwise change the Internet filtering software or other network configurations.
- 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, or vulgar images, sounds, music, language, video, or other materials. The criteria for acceptability is demonstrated in the types of material made available to students by administrators, teachers, and the school media center. Specifically, all district-owned technologies should be free at all times of any pornographic, obscene, graphically violent, or vulgar images, sounds, music, language, video, or other materials (files).
- Will keep computing devices secure and damage free.
- Will back up data and other important files regularly. WCSD will at times maintain the devices by imaging. All files not backed up to server storage space or other storage media will be deleted during these processes. Students and staff are ultimately responsible for backing up all personal files on their own storage media.

Follow these general guidelines for school-issued devices:

- Do not loan your device, charger, cords, or any other device-related items.
- Do not leave the device in a vehicle.
- Do not leave your device unattended.
- Do not eat or drink while using the device or have food or drinks near the device.
- Do not allow pets near your device.
- Do not place the device on the floor or sit in areas such as couches or chairs.
- Do not leave the device near a table or desk edges.
- Do not stack objects on top of your device.
- Do not leave the device outside or use it near water, such as a pool.
- Do not check the device as luggage at the airport.
- Devices should be securely stored and not in use when walking in the hall.