Waltonville CUSD 1
Authorization for Electronic Network Access 2019-2020

All use of electronic networks must be consistent with the school's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. These rules do not attempt to state all required or proscribed behavior by users. However, some specific examples are provided. **The failure of any user to follow these rules will result in the loss of privileges, disciplinary action, and/or appropriate legal action.**

Acceptable Use - Access to the electronic network must be: (a) for the purpose of education or research, and be consistent with the District's educational objectives, or (b) for legitimate business use.

Privileges - The use of the electronic network is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. The system administrator or Building Principal will make all decisions regarding whether or not a user has violated these procedures and may deny, revoke, or suspend access at any time. His or her decision is final.
Consequences of violations include, but are not limited to:

- Suspension/revocation of Internet access
- Suspension/revocation of network privileges
- Suspension/revocation of computer access
- Detention
- In-school or out-of-school suspension
- Recommendation for expulsion
- Legal action/prosecution by authorities

Unacceptable Use - The user is responsible for his or her actions and activities involving the network. Some examples of unacceptable uses are,

1. Using the network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any State or federal law;
2. Unauthorized downloading of software, regardless of whether it is copyrighted or de-virused;
3. Downloading of copyrighted material for other than personal use;
4. Using the network for private financial or commercial gain;
5. Wastefully using resources, such as file space;
6. Hacking or gaining unauthorized access to files, resources, or entities;
7. Invading the privacy of individuals, that includes the unauthorized disclosure, dissemination, and use of information about anyone that is of a personal nature including a photograph;
8. Using another user's account or password;
9. Posting material authored or created by another without his/her consent;
10. Posting anonymous messages;
11. Using the network for commercial or private advertising;
12. Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material; and
13. Using the network while access privileges are suspended or revoked.
14. Sending or displaying offensive messages or pictures
15. Harassing, insulting, attacking, or threatening others
16. Using another user's password
17. Trespassing in another user's folder, work, or files

Network Etiquette - The user is expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

1. Be polite. Do not become abusive in messages to others.
2. Use appropriate language. Do not swear, or use vulgarities or any other inappropriate language.
3. Do not reveal personal information, including the addresses or telephone numbers, of students or colleagues.
4. Recognize that electronic mail (e-mail) is not private. People who operate the system have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities.
5. Do not use the network in any way that would disrupt its use by other users.
6. Consider all communications and information accessible via the network to be private property.

No Warranties - The school and district make no warranties of any kind, whether expressed or implied, for the service it is providing. The school and district are not responsible for any damages the user suffers. This includes loss of data resulting from delays, non-deliveries, missed-deliveries, or service interruptions caused by its negligence or the user's errors or omissions. Use of any information obtained via the Internet is at the user's own risk. The school and district specifically deny any responsibility for the accuracy or quality of information obtained through its services.

Indemnification - The user agrees to indemnify the school and district for any losses, costs, or damages, including reasonable attorney fees, incurred by the school or district relating to, or arising out of, any violation of these procedures.

Security - Network security is a high priority. If the user can identify a security problem on the Internet, the user must notify the system administrator or building principal. Keep your account and password confidential. Do not use another individual's account without written permission from that individual. Any user identified as a security risk may be denied access to the network.
Quality Network Systems provides and maintains the content filtering application on Internet access and the e-mail spam filtering application. Updates are monitored on a daily basis by QNS. Daily monitoring by QNS as well the administration or designee address the following measures: (1) limiting student access to inappropriate matter, (2) restricting student access to materials harmful to them, (3) ensuring student safety and security when using electronic mail, chat rooms, and other forms of electronic communications, (4) limiting unauthorized access, including "hacking" and other unlawful activities by minors online; and (5) limiting unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

Vandalism - Vandalism will result in cancellation of privileges and other disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, or any other network. This includes, but is not limited to, the uploading or creation of computer viruses.

Plagiarism – Plagiarism is defined as "taking ideas or writings from another person and offering them as your own". Credit must always be given to the person who created the article or the idea. Users, who lead readers to believe that what they are reading is the user's original work, when it is not, are guilty of plagiarism. The Student Handbook policy on cheating and academic dishonesty, including plagiarism, shall be applied to District computer use.

Copyright Web Publishing Rules - Copyright law prohibits the republishing of text or graphics found on the Web without explicit written permission.

1. For each re-publication (on a Web site or file server) of a graphic or a text file that was produced externally, there must be a notice at the bottom of the page crediting the original producer and noting how and when permission was granted. If possible, the notice should also include the Web address of the original source.
2. Students engaged in producing Web pages must provide the teacher and/or staffs with e-mail or hard copy permissions before the Web pages are published. Printed evidence of the status of “public domain” documents must be provided.
3. The absence of a copyright notice may not be interpreted as permission to copy the materials. Only the copyright owner may provide the permission. The manager of the Web site displaying the material may not be considered a source of permission.