Charleston Community Unit School #1
Acceptable Use Procedure (AUP) for Access to the District's Electronic Networks

Charleston CUSD #1 instructional programs are designed to ensure that users become proficient in information and communication technologies (ICT) essential for their success. All use of the District's electronic networks shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation and communication. These procedures do not attempt to state all required or prescribed behavior by users. However, some specific examples are provided. The failure of any user to follow these procedures will result in disciplinary action, limitation or loss of privileges and/or appropriate legal action.

Terms and Conditions

1. **Acceptable Use** - Access to the District's electronic networks 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.

2. **Privileges** - Use of the District's electronic networks is a privilege, not a right, and inappropriate use may result in disciplinary action, limitation or loss of those privileges and/or appropriate legal action. Administration 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.

3. **Safety/Security Measures** - Network safety and security is a high priority. If a user can identify a safety/security problem on the Network, the user must notify building staff or the system administrator. Do not demonstrate the problem to other users. Keep your account and password confidential. Do not use another individual's account without written permission from that individual. Attempts to log-on to the Network as a system administrator will result in cancellation of user privileges. Any user who receives any harassing, threatening, intimidating or other improper communication through the District's electronic networks is urged to report it immediately. Any user identified as a security risk may be denied access to the networks.

   A. Filtering
   - District electronic networks have a filtering device that blocks language, sites and visual depictions that are (1) obscene, (2) pornographic, or (3) harmful or inappropriate for users, as defined by the Children's Internet Protection Act and as determined by the Superintendent or his/her designee.

   B. Monitoring
   - The District reserves the right to monitor and access all use of or content on the District's technologies and networks. Users have no expectation of privacy when using district electronic networks including information created, received, transmitted and stored on these resources unless such right is guaranteed by statute or other law.

   C. Supervision
   - Charleston CUSD #1 staff will be responsible for supervising all users on District electronic networks.

   D. Education
   - Education about online safety and digital citizenship (online behavior, communication, cyber-bullying, literacy, etiquette, rights and responsibilities and security) will be covered in the K-12 curriculum each school year.

4. **Unacceptable Use -** The user is responsible for his or her actions and activities involving the networks. Some examples of unacceptable uses are:
   A. Using the networks for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any State or federal law;
   B. Downloading, installing, and use of unauthorized software, regardless of whether it is copyrighted or de-virused;
   C. Downloading of copyrighted material for other than personal use;
   D. Using the networks for private financial or commercial gain and/or advertising;
   E. Wastefully using resources, such as bandwidth and file space;
   F. Hacking, or gaining unauthorized access to files, resources or entities bypassing or attempting to circumvent security, virus protection, filtering, or policies;
   G. 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;
   H. Sharing or using another user's account and password;
   I. Posting material authored or created by another without his/her consent;
   J. Posting anonymous messages
   K. Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material; and
   L. Using the networks while access privileges are suspended or revoked.

5. **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:
   A. Be polite. Do not become abusive in messages to others.
   B. Use appropriate language. Do not swear or use vulgarities or any other inappropriate language.
   C. Do not reveal personal information, including the addresses or telephone numbers, of yourself or others.
   D. Recognize that email is not private. People who operate the system have access to all email. Messages relating to or in support of illegal activities may be reported to the authorities.
   E. Do not use the networks in any way that would not disrupt the educational process or the normal operations of the District.
   F. Consider all communications and information accessible via the networks to be private property.

6. **No Warranties** - The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages an individual 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 a user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services. It is the user's responsibility to make backups of their data and email.

7. **Indemnification** - The user agrees to indemnify the School District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of, any breach of this Procedure.

8. **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, attempting to vandalize or harm data and/or disconnect or disassemble any technology.

9. **Online/Telephone Charges** - The District assumes no responsibility for any unauthorized charges or fees, including telephone charges, long-distance charges, per-minute surcharges, equipment, line or data costs and online purchases.

10. **Copyright, Fair Use and Publishing Guidelines** - Copyright laws, fair use guidelines and District policy prohibit the re-publishing of text or graphics found on the web or on District websites or file servers without explicit written permission.
    A. 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 website displaying the material may not be considered a source of permission.
    B. The *fair use* rules governing student reports in classrooms are less stringent and permit limited use of graphics and text.
    C. Additional guidelines specific to web publishing in Policy 6:235-AP2 are identified and should be followed.

11. **User Work/Photos/Videos -** User work, photos and/or videos may be published on District web pages upon receipt of this agreement unless the user or guardian (if the user is a minor) notifies the school otherwise. Users whose work, photo and/or video appear on the District/school web page(s) will be identified by first name only.

12. **Use of Email –** The School District provides email to aid students and staff members in fulfilling their duties and responsibilities, and as an education tool.
    A. The District reserves the right to access and disclose the contents of any account on its system, without prior notice or permission from the account's user. Unauthorized access by any student or staff member to an email account is strictly prohibited.
    B. Each person should use the same degree of care in drafting an email message as would be put into a written letter or document. Nothing should be transmitted in an email message that would be inappropriate in a letter or document.
    C. User accounts are identified with a domain that indicates the author as being with the District. Great care should be taken, therefore, in the composition of such messages and how such messages might reflect on the name and reputation of the District. Users will be held personally responsible for the content of any and all email messages transmitted to external recipients.
    D. Any message received from an unknown sender via the Internet should be immediately deleted. Downloading any file attached to any Internet-based message is prohibited unless the user is certain of that message's authenticity and the nature of the files so transmitted.
    E. Use of the School District's email system constitutes consent to these regulations.
    F. The District's student email system limits with whom the students can communicate~~s.~~ with.
    G. Student email accounts are not private in nature. Designated staff may monitor, inspect and review at any time and without prior notice any information in all accounts.

ADOPTED: July 19, 2017