Acceptable Usage Policy for Student Network and Internet Access

2021-2022 School Year

Each student and his or her parent(s) must sign this Authorization each school year before being granted access to the Brown County Community Unit School District #1 (hereafter referred to as "District") computer network and Internet connection. Each user must sign this Authorization each school year as a condition for using the District's computer network and Internet connection.

Please read this document carefully before signing.

All use of the network and Internet connection shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. The Terms and Conditions set forth below are designed to comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)]. This Authorization does not attempt to state all required or proscribed behavior for users. However, some specific examples are provided. The failure of any user to follow the terms of the Acceptable Usage Policy for Network and Internet Access will result in the loss of computer and network privileges, disciplinary action, and legal action as deemed appropriate by District administrators. In this document "network" is meant to include any aspect of any computer network, hardware or software in the District. In the case of the Internet, network means any aspect of any network, computer, hardware or software. The signature(s) at the end of this document indicate those who have signed have read the terms and conditions carefully and understand their significance.

Terms and Conditions

1. Acceptable Use - Access to the District's network and the Internet connection must be for the purpose of education or research, and be consistent with the educational objectives of the District.
2. Privileges - The use of the District's network and Internet connection is a privilege, not a right. The system administrators and District administrators will make all decisions regarding whether or not a user has violated any of the rules of usage, and may deny, revoke, or suspend access at any time.
3. Unacceptable Use - You are responsible for your actions and activities involving computers and the network. Some examples of unacceptable uses are:
    a. Using the network for any illegal activity, including violation of copyright or contracts, or transmitting any material in violation of any U.S. or State regulation or District rule;
    b. Unauthorized installation of software, regardless of whether it is copyrighted or virus-free;
    c. Using material in violation of copyright, except as is permitted by law as "fair use";
    d. Using the computers or network for private financial or commercial gain;
    e. Wastefully using computer or network resources, such as file space, or bandwidth or unnecessary/wasteful printing, or any other use that has the purpose or effect of using more network resources than is permitted or necessary for the user's purposes.
    f. Gaining unauthorized access to resources or entities, whether internal or external to the District, by any means;
    g. Gaining access to others' folders, work, or files, or changing files or settings not belonging to the user, including but not limited to, desktop icons, wallpapers, screensavers, or default settings;
    h. Invading the privacy of individuals;
    i. Using another user's account or password;
    j. Providing another user's account or password to someone else;
    k. Posting material authored or created by another without his/her consent;
    l. Posting anonymous messages;
    m. Using a school e-mail account for non-school communication (social media, subscriptions, etc.);
    n. Using the network for advertising;
    o. Accessing, submitting, posting, publishing or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal messages, pictures, or other material;
    p. Using the network while access privileges are suspended or revoked;
    q. Disseminating confidential information including, but not limited to, account passwords and Wi-Fi passwords;
    r. Changing permissions on files and/or folders residing on the network or local computers;
    s. Attempting to bypass Internet filtering to gain access to a restricted site;
    t. Copying music from removable media (CD, flash drive, etc.) or a personal device (phone, MP3 player, etc.) to the network or downloading music from the Internet for non-educational purposes. Examples of educational uses include class projects and assignments where the use has been approved by the teacher.
4. Network Etiquette - You are 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 your messages to others.
    b. Use appropriate language. Do not swear or use vulgarities or any other inappropriate language.
    c. Do not reveal the personal addresses or telephone numbers of others.
    d. Do not use the network in any way that would disrupt its use by other users.
5. The District owns the rights to all data and files in any computer, network, or other information system or storage device owned or subscribed to by the District. The District also reserves the right to monitor electronic mail messages and their content and attachments. Users should be aware that the files and electronic mail messages that they create, use, send or receive using the network are not private and are subject to viewing, downloading, inspection, release, and archiving by District officials at all times. Use relating to or in support of illegal activities may be reported to the authorities. No user may access another user's computer, computer files, or electronic mail messages without prior authorization from either the user or an appropriate District official.
6. Internet and network use is not confidential and no rights to privacy exist. The District reserves the right to monitor Internet and network usage, both as it occurs and in the form of account histories and their content. The District has the right to inspect any and all files stored on the network or within any subscribed services in order to assure compliance with policy and state and federal laws. The District will comply with reasonable requests from law enforcement and regulatory agencies for logs, diaries, archives, and/or files on individual Internet activities to the extent permitted by law. Other rules, policies and procedures governing the academic honesty, and release of work-

related or other confidential information also apply to the sharing of information via the network Internet.

7. Personal Devices - Although the District utilizes a Bring Your Own Device program, students are not permitted to connect their personal device to any network that is not maintained by the District while they are present at school. This includes, but is not limited to, mobile hotspot networks or other wireless networks that may be available.
8. No Warranties - The District makes no warranties of any kind, whether expressed or implied, regarding the network, Internet or the service it is providing. The District will not be responsible for any damages you suffer arising out of, or in connection with use of the network or Internet. This includes loss of data resulting from delays, non-deliveries, missed deliveries, or service interruptions caused by its negligence or your errors or omissions. Use of any information obtained via the Internet is at your own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.
9. 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 policy by the user.
10. Security - The District has taken reasonable precautions intended to provide the safety and security of the network, both internally and externally, from unauthorized access (including hacking). These measures, among other things, are intended to protect against the unauthorized access to personal and private information. Any user who attempts to disable, defeat, or circumvent District security measures is subject to disciplinary action. If you can identify a security problem on the network, you must notify the system administrators or the Building Principal. Do not demonstrate the problem to other users.
11. Keep your account and password confidential. Unauthorized attempts to log on to the network as a system administrator will result in cancellation of user privileges and recommendation to the Board of Education for expulsion. Any user identified as a security risk may be denied access to the network.
12. Internet Safety - The District has taken reasonable precautions intended to provide the safety of students from material which may be harmful to minors, including obscene or pornographic material. These precautions include but are not limited to, the filtering and monitoring of: web sites, e-mail, chatting/instant messaging, and social communities (such as Facebook). All usage of the network is filtered and monitored. Teachers are also responsible for monitoring real-time network and Internet usage by students in the classroom and lab and educating students on safe and responsible use.
13. 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 connection, or any other network component, including, but not limited to, the creation or uploading of computer viruses or other malware. Vandalism is also defined as any malicious attempt to harm or destroy computer equipment, including but not limited to the monitor, keyboard, mouse, CPU, cables, printers.
14. Charges - The District assumes no responsibility for any unauthorized charges or fees, including telephone charges, long-distance charges, per-minute surcharges, and/or equipment or line costs.
15. Off-Campus Conduct - The District may discipline students whose off-site activity involving electronic technology cause, or can reasonably be expected to cause, a substantial disruption of the school environment or the District network or Internet connection, without regard to whether that activity or disruption involved use of the District network or Internet connection. Cyberbullying – Bullying is generally defined as unwanted aggressive behavior by a person or persons directed toward another person or persons which involves a real or perceived power imbalance.
16. Cyberbullying is bullying using electronic technology. Electronic technology includes devices and equipment such as cell phones, computers and tablets, as well as communication tools, including social media sites, text messages, chat and websites. Examples of cyberbullying include mean text messages or e-mail, rumors sent by e-mail or posted on social networking sites and embarrassing pictures, videos, websites or fake profiles. Cyberbullying which has an adverse impact on the school setting will be subject to disciplinary action by school authorities even if such cyberbullying takes place after school hours and off school property.

Students, and parent(s)/guardian(s) are required to sign this Authorization every year while enrolled in the School District in order to have access to the District network or Internet Connection.

I understand and will abide by the above *Acceptable Usage Policy for Network and Internet Access.* I further understand that should I commit any violation, my access privileges will be revoked, and school disciplinary action and legal action will be taken. In consideration for using the District's computer network and Internet connection, and having access to public networks, I hereby release the School District and its Board members, employees, and agents from any claims and damages arising from my use, or inability to use the network and Internet connection.

The following must be filled out by a parent/guardian of the student:

I have read this *Acceptable Usage Policy for Network and Internet Access.* I understand that access is designed for educational purposes and that the District has taken the precautions described above. However, I also recognize that 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 or Internet connection. I accept full responsibility for supervision if and when my child's use is not at the District. I have discussed the terms of this *Acceptable Usage Policy for Network and Internet Access* with my child. I hereby request that my child be allowed access to the District's computer network and Internet connection.

Student's Name (Please print): _____

Parent/Guardian's Name (Please print): _____

Parent/Guardian's Signature: _____

Date_____ **Student Grade Level_____**