Authorization for Electronic Network Access Form

Submit to Building Principal.

I understand and will abide by the below *Acceptable Use Policy*. I understand that the District and/or its agents may access and monitor my use of the Internet, including my E-mail and downloaded material, without prior notice to me. I further understand that should I commit any violation, my access privileges may be revoked, and school disciplinary action and/or appropriate legal action may be taken. In consideration for using the District's electronic network 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 of, or inability to use the Internet.

User's Name: ________________________________

Signature: ________________________________ Date: _________________

***Students are required to have a parent/guardian read and agree to the following:**

I have read this *Acceptable Use Policy*. 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 accept full responsibility for supervision if and when my child's use is not in a school setting. I have discussed the terms of this Authorization with my child. I hereby request that my child be allowed access to the district's Internet.

Parent/Guardian Name: ________________________________

Signature: ________________________________

Date: ____________________

Jasper County School District
Acceptable Use Policy

Introduction

Jasper County School District recognizes that access to technology in school gives students greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship. We are committed to helping students develop 21st century technology and communication skills.

To that end, we provide the **privilege** of access to technologies for student and staff use.

This Acceptable Use Policy outlines the guidelines and behaviors that students and staff are expected to follow when using school technologies or when using personally-owned devices on the school campus.

- The District network is intended for educational purposes.
- All activity over the network or using district technologies may be monitored and retained.
- Access to online content via the network may be restricted in accordance with our policies and federal regulations, such as the Children's Internet Protection Act (CIPA).
- Students are expected to follow the same rules for good behavior and respectful conduct online as offline.
- The District makes a reasonable effort to ensure students' safety and security online, but will not be held accountable for any harm or damages that result from use of school technologies.
- Users of the district network or other technologies are expected to alert IT staff immediately of any concerns for safety or security.
- **Failure to adhere to the terms of this Acceptable Use Policy will result in disciplinary action**, as detailed at the end of this document.

Technologies Covered

The District may provide Internet access, desktop computers, mobile computers or devices, videoconferencing capabilities, online collaboration capabilities, email, and more.

As new technologies emerge, the District will attempt to provide access to them. The policies outlined in this document are intended to cover *all* available technologies, not just those specifically listed.

Usage Policies

All technologies provided are intended to further the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. All users are expected to use good judgment and to follow the specifics of this document as well as the spirit of it: be safe, appropriate, careful and kind; don't try to get around technological protection measures; use good common sense; and ask if you don't know.

Web Access

The District provides its users with access to the Internet, including web sites, resources, content, and online tools.

Users are expected to respect that the web filter is a safety precaution, and should not try to circumvent it when browsing the Web. If a site is blocked and a user believes it shouldn't be, the user should follow district protocol to alert an IT staff member or submit the site for review.

Staff members shall supervise students while students are using District Internet access to ensure that the students abide by the Terms and Conditions for Internet access contained in this Authorization.

Each District computer with Internet access has a filtering device that blocks entry to visual depictions that are: (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by the Children's Internet Protection Act and as determined by the Superintendent or designee.

The IT staff and Building Principals shall monitor student Internet access.

Email

The School District provides email to aid students and staff members in fulfilling their duties and responsibilities, and as an educational tool. If users are provided with email accounts, they should be used with care. Users should not send personal information; should not attempt to open files or follow links from unknown or untrusted origin; and should use appropriate language. Students should only use District accounts to communicate with approved sources.

Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Users should recognize that email is not private; email messages may be monitored and archived. Messages relating to or in support of illegal activities may be reported to the authorities.

Social Media / Web 2.0 / Collaborative Content

Recognizing the benefits collaboration brings to education, the District may provide users with access to web sites or tools that allow communication, collaboration, sharing, and messaging among users.

Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Posts, chats, sharing, and messaging may be monitored. Users should be careful not to share personally-identifying information online.

Mobile Devices Policy

The District may provide users with mobile computers or other devices to promote learning outside of the classroom. Users should abide by the same acceptable use policies when using school devices off the school network as on the school network.

Users are expected to treat these devices with extreme care and caution; these are expensive devices that the school is entrusting to your care. Users should immediately report any loss, damage, or malfunction to IT staff . Users may be financially accountable for any damage resulting from negligence or misuse.

Use of school-issued mobile devices off the school network may be monitored.

Bring Your Own Device Policy

The District is committed to aiding students and staff in creating a 21st century learning environment. Many schools in the nation are implementing Bring Your Own Device policies for their students and staff. Students at NCHS and JCJH and staff will now be able to access our wireless network with their personal devices (laptops, netbooks, tablets, smartphones, etc) during the school day. By allowing these students to use their own technology in school, we are hoping to increase the access all students have to the technology they need to succeed. With classroom teacher approval. students may use their own devices to access the Internet and collaborate with other students.

For further information, please reference the JCCU1 BYOD document.

Security

Network security is a high priority. If you identify a security issue on the network, you must notify the IT department or building principal. Do not demonstrate the problem to other users. Keep your account and password confidential. Attempts to gain unauthorized access to systems will result in disciplinary action.

Users are expected to take reasonable safeguards against the transmission of security threats over the school network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin.

If you believe a computer or mobile device you are using might be infected with a virus, please alert IT. Do not attempt to remove the virus yourself or download any programs to help remove the virus.

Downloads

Users should not download or attempt to download or run unauthorized programs over the school network or onto school resources without express permission from IT staff.

You may be able to download other file types, such as images of videos. For the security of our network, download such files only from reputable sites, and only for educational purposes.

Netiquette

Users should always use the Internet, network resources, and online sites in a courteous and respectful manner.

Users should also recognize that among the valuable content online is unverified, incorrect, or inappropriate content. Users should use trusted sources when conducting research via the Internet.

Users should also remember not to post anything online that they wouldn’t want parents, teachers, or future colleges or employers to see. Once something is online, it’s out there—and can sometimes be shared and spread in ways you never intended.

Plagiarism

Users should not plagiarize (or use as their own, without citing the original creator) content, including words or images, from the Internet. Users should not take credit for things they didn’t create themselves, or misrepresent themselves as an author or creator of something found online. Research conducted via the Internet should be appropriately cited, giving credit to the original author.

Personal Safety

Users should never share personal information, including phone number, address, social security number, birthday, or financial information, over the Internet without express permission. Users should recognize that communicating over the Internet brings anonymity and associated risks, and should carefully safeguard the personal information of themselves and others. Users should never agree to meet someone they meet online in real life without parental permission.

If you see a message, comment, image, or anything else online that makes you concerned for your personal safety, bring it to the attention of an adult (teacher or staff if you’re at school; parent if you’re using the device at home) immediately.

Cyberbullying

Cyberbullying will not be tolerated. Harassing, disrespecting, flaming, denigrating, impersonating, outing, tricking, excluding, and cyberstalking are all examples of cyberbullying. Do not send emails or post comments with the intent of scaring, hurting, or intimidating someone else.

Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges. In some cases, cyberbullying can be a crime. Remember that your activities are monitored and retained.

Examples of Acceptable Use

I will:

- Use school technologies for school-related activities.
- Follow the same guidelines for respectful, responsible behavior online that I am expected to follow offline.
- Treat school resources carefully, and alert staff if there is any problem with their operation.
- Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
- Alert a teacher or administrator if I see threatening, inappropriate, or harmful content (images,

messages, posts) online.

- Use school technologies at appropriate times, in approved places, for educational pursuits.
- Cite sources when using online sites and resources for research.
- Recognize that use of school technologies is a privilege and treat it as such.
- Be cautious to protect the safety of myself and others.
- Help to protect the security of school resources by alerting IT staff to potential issues.

This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies.

Examples of Unacceptable Use

I will **not**:

- Use school technologies in a way that could be personally or physically harmful.
- Attempt to find inappropriate images or content.
- Engage in cyberbullying, harassment, or disrespectful conduct toward others.
- Try to find ways to circumvent the school's safety measures and filtering tools.
- Use school technologies to send spam or chain mail.
- Use another user's account.
- Plagiarize content I find online.
- Post personally-identifying information, about myself or others.
- Agree to meet someone I meet online in real life.
- Use language online that would be unacceptable in the classroom.
- Use school technologies for illegal activities or to pursue information on such activities.
- Use the network for private financial or commercial gain
- Attempt to 'hack' or access sites, servers, or content that isn't intended for my use.

This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies.

Limitation of Liability

The District will not be responsible for damage or harm to persons, files, data, or hardware.

While the District employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness.

The District will not be responsible, financially or otherwise, for unauthorized transactions conducted over the school network.

The District specifically denies any responsibility for the accuracy or quality of information obtained through it services; use of any information obtained via the Internet is at the user's own risk.

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.

Violations of this Acceptable Use Policy

Violations of this policy may have disciplinary repercussions. Please refer to the student handbook, Board Policy and Collective Bargaining Agreement (certified employees only) for explanations of due process and disciplinary action. The superintendent or designee will make all decisions regarding whether or not a user has violated the terms of this policy.