Colville School District
Acceptable Use Policy

1. Purpose

This Acceptable Use Policy is intended to support the policies of the Colville School District and to promote positive and effective digital citizenship among students and staff. Digital citizenship represents more than technology literacy. Successful, technologically fluent digital citizens live safely and civilly in an increasingly digital world. They recognize that information posted on the Internet is public and permanent and can have a long-term impact on an individual's life and career. Student and staff behavior online must comply with District and school rules and maintain appropriate professional student/teacher boundaries at all times. Failure to comply with the rules of this Policy shall subject the staff or student to disciplinary action, which is not limited to denying access to District technology, and may include termination for staff or expulsion for students, depending upon the severity of the misconduct.

2. Acceptable Use

Acceptable uses of District technology are those that support the operational requirements and educational purposes in creating enhanced learning opportunities for students, such as:

- Creation of files, digital projects, videos, web pages, and podcasts using network resources in support of education and research;
- Participation in social networking and the creation of content for podcasts, email, and web pages that support education and research;
- With parental permission, the online publication of original educational material, curriculum-related materials, and student work;
- Staff use of the network for incidental personal use in accordance with all District policies and procedures;
- Connection of approved personal electronic devices to the District network. Connection of any personal electronic device is subject to all policies and procedures in this document.

The use of District technology resources is a privilege, and not a right.

3. Unacceptable Use

Unacceptable uses of District technology are those that do not support operational requirements or educational purposes for students. Unacceptable uses include, but are not limited to:

- Circumventing or disabling the District's filtering or monitoring systems or any other security measures;
- Gaining access to computer or network resources using another's credentials;
- Creating a fictitious identity or impersonating another;
- Gaining unauthorized access to hardware, software, and security or monitoring tools;
- Furthering personal causes, such as political (including District Levy or Bond initiatives)

or religious views or personal financial gain;
- Taking actions that result in liability or cost incurred by the District;
- Invading the privacy of another person, including obtaining, copying, and modifying files, passwords, data, or information belonging to another user;
- Disclosing, using or disseminating the personal information of another;
- Downloading and/or installing unauthorized or illegal software, files, or programs;
- Purposefully or recklessly infecting the network or computers with spyware, malware, or viruses or vandalizing District equipment;
- Disseminating threatening or harassing messages (cyberbullying) or discriminatory jokes or remarks;
- Accessing, disseminating, or storing material that could endanger self or others (e.g., weapons, drug manufacturing);
- Accessing, disseminating, or storing obscene, pornographic, sexually explicit, or other inappropriate material, whether on District-owned devices or on personal devices used on the District network;
- Using District resources to encourage or advocate illegal or violent activities or discrimination towards other individuals or groups;
- Attaching unauthorized devices to the District network, including creating unauthorized wireless access points.

4. Content Filtering & Monitoring

The Colville School District uses software designed to block access to certain sites and filter content as required by the Children's Internet Protection Act (CIPA). Though the District makes reasonable efforts to filter Internet content, the District cannot guarantee the effectiveness of Internet filtering due to the dynamic nature of the Internet. However, the District will make an effort to correct any known gaps in the filtering of information without unduly inhibiting the education use of age-appropriate content by staff and students.

- The District will provide appropriate adult supervision of students' Internet use;
- Staff members who supervise students, control electronic equipment, or have occasion to observe student use of equipment must make reasonable efforts to monitor the use of this equipment to assure that student use conforms to the mission and goals of the District;
- Staff must make reasonable efforts to become familiar with the Internet and to monitor, instruct, and assist effectively;
- The District will provide a procedure for students and staff to request access to Internet websites blocked by the District's filtering software. The requirements of the Children's Internet Protection Act (CIPA) will be considered in evaluation of the request;
- Email inconsistent with the educational and research mission of the District may be considered spam and be blocked from entering District email boxes.

5. Archive & Backup

All District email correspondence is regularly backed up for the purposes of public disclosure and disaster recovery. Barring power outage or intermittent technical issues, staff and student files are backed up on District servers regularly.

6. Safety & Security

Students and staff are responsible for keeping their personal information private. They will:

- Not reveal personal information, including names, home, work, or school addresses; phone numbers, or email addresses, about yourself or others on websites, blogs, podcasts, videos, social networking sites, wikis, email, or as content on any other electronic medium;
- Not publish student names or pictures on any public class, school, or District website without appropriate permission as according to District policy;
- Notify the appropriate school authority of they encounter dangerous or inappropriate information or messages;
- Never arrange meetings with anyone they have met online without the knowledge of the school and permission of a parent or guardian;
- Promptly disclose to teachers or administrators any messages they may receive that are inappropriate, threatening, unwelcoming, or make them feel uncomfortable.

Staff and students are responsible for all activity on their individual access accounts and should take all reasonable precautions to prevent others from being able to use their accounts, including coworkers, friends, or family. They will:

- Not reveal password(s) to other individuals;
- Change passwords according to District policy;
- Not use another's account;
- Not include passwords in email or other communications;
- Store any written-down passwords in a secure location;
- Not store passwords in a computer file without encryption;
- Lock the screen or log off if leaving the computer.

Passwords used on the District's system are the property of the District and must be provided to an administrator, supervisor, or designated District personnel, as requested.

7. Expectations of Privacy

The District provides the network system, email, and Internet access as tools for education and research in support of the District's mission. The District reserves the right to monitor, inspect, copy, review, and store without prior notice information about the content and usage of:

- The network;
- User files and disk space utilization;
- User applications and bandwidth utilization;

- User document files, folders and electronic communications;
- Email;
- Internet access;
- Any and all information transmitted or received in connection with network and email use;
- District phone system and voicemails stored on the phone system.

The District may also be able to confiscate and search personal electronic devices used on the District network or used to access District resources.

No student or staff user should have any expectation of privacy when using the District's network or accessing District resources. The District reserves the right to disclose any electronic messages to law enforcement officials or third parties as appropriate. All records may be subject to disclosure to the public under the Washington Public Records Act.

8. Google Applications for Education (GAfE)

Google Applications for Education is available to all staff, faculty members, and students in grades K through 12. Email that originates from or is received by a District-owned computer, or its contracted Google Apps for Education, is the property of the Colville School District and can be used for or against during a legal proceeding.

Google Apps for Education, including associated sites, email, and groups, is not a public forum. Use of Google Apps for Education is an extension of classroom spaces where free speech rights may be limited. District staff and administrators have access to student email and files for monitoring purposes. There should be no expectation of privacy on the Google Apps for Education system.

- When writing or responding via email, all users of the District's email system should remember that emails creates a record and all records, even personal communication, may be subject to public disclosure under the Washington Public Records Act (Chapter RCW 42.56). All Google accounts, including student accounts, are the property of the Colville School District.
- Student accounts will be deleted in August of their graduation year and students are solely responsible for transferring any data in their accounts to personal, non-District-owned accounts.
- Use of the District's Google account is a privilege, not a right.
- Use of the District Google student accounts aligns with the student handbook's code of conduct, and the code will be used for discipline purposes.
- Students are responsible for the content of messages sent from their accounts.
- Students should exercise extreme caution with their passwords and never let others use their accounts.
- No students or staff shall use District Google accounts to operate a personal business.
- The District reserves the right to either temporarily or permanently terminate a Google account if used inappropriately. A student shall be entitled to utilize District and

regulatory grievance processes (WAC Chapter 392-400) to dispute the denial of access. Access denial continues during the grievance process at the discretion of the Principal or designee.

- Students will not provide their personal telephone numbers, home addresses, or any personal information in any email correspondence.
- No expectation of privacy should be assumed when using District-assigned Google accounts. The District administrative and technology staff reserve the right to access users' mailboxes and storage drive to find lost messages, to conduct lawful investigations, or to comply with investigations of wrongful acts. The District will cooperate fully with any law enforcement investigation. Illegal activities on the system will be referred to law enforcement authorities for appropriate legal action.
- The Colville School District reserves the right to change providers without prior notice.
- Following usage of a Google Apps for Education account, the user will log off so as to prevent another user from using his/her account.
- Since the District-assigned Google accounts can be accessed outside the boundaries of our schools (web-based accounts) students and staff are required to maintain the same online behavior while accessing their accounts off-campus that is expected of them while accessing their accounts on school premises.

School staff will monitor student use of Google Apps for Education when students are at school. Parents are responsible for monitoring their child's use when accessing programs from home or non-school locations. Students are responsible for their own behavior at all times.

9. Copyright & Plagiarism

Downloading, copying, duplicating and distributing software, music, sound files, movies, images or other copyrighted materials without the specific written permission of the copyright owner is generally prohibited. However, the duplication and distribution of legally obtained materials for educational purposes is permitted when such duplication and distribution falls within the very limited Fair Use Doctrine of the United States Copyright Law (Title 17, USC) and content is cited appropriately.

All sources, references, and quoted material will be cited appropriately. Acknowledging the source of copyrighted material does not substitute for obtaining reproduction rights. Users are responsible for ensuring they are in compliance with copyright protections and should err on the side of not using the material if "fair use" is in question.

10. Confidential Student Records

Student records are confidential and protected by the Family Educational Rights and Privacy Act (FERPA). It shall be inappropriate for anyone to disclose the records of a student in violation of
FERPA or Washington State Law (RCW28A.605.030) prohibiting disclosure without parental consent.

11. Etiquette

Users are expected to abide by the generally accepted rules of network etiquette. This includes, but is not limited to:

- Being polite. Respect the rights of others to an open and hospitable technology environment, regardless of race, sexual orientation, gender identity, color, religion, creed, ethnicity, age, marital status, or handicap status.
- Using appropriate language. Use of profanity, vulgarities, inflammatory, lewd, or abusive language is prohibited.
- Exercising caution when using sarcasm or humor. Without the additional non-verbal information provided by face-to-face communication, jokes or statements may be misunderstood.
- Respecting others' privacy. Do not share private messages or information on web pages, cell phones, or other devices.