Coeur d'Alene School District No. 271

STUDENTS **3270P**

Acceptable Use of Electronic Networks

All use of 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 proscribed behaviors by users. However, some specific examples are provided. **The failure of any user to follow these procedures will result in the loss of privileges, disciplinary action, 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 consistent with the educational objectives of the District; or
   B. For legitimate business use.

2. Use is a privilege, not a right. Students' freedom of speech and access to information will be honored. However, students have no expectation of privacy in any materials that are stored, transmitted, or received via the District's electronic network or District computers. The District reserves the right to access, monitor, inspect, copy, review, and store, at any time and without prior notice, any and all usage of the computer network and internet access and any and all information transmitted or received in connection with such usage, including email and instant messages.

   The system administrators will not intentionally inspect the contents of e-mail sent by one user to an identified addressee, or disclose such contents to other than the sender, or an intended recipient, without the consent of the sender or an intended recipient, unless required to do so by law or by policies of this District, or to investigate complaints regarding e-mail which are alleged to contain defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal material.

3. Privileges: The use of the District's electronic networks is a privilege, not a right, and inappropriate use will result in cancellation of those privileges. The Internet Safety Coordinator, in conjunction with the System Administrator and the 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. An appeal of such decisions may be made to the Superintendent within seven (7) days. His or her decision is final.

4. Unacceptable Uses: The user is responsible for his or her actions and activities involving the network. Some examples of unacceptable uses are the following. Additional unacceptable uses can occur other than those specifically listed or enumerated herein:

A. Uses that violate the law or encourage others to violate the law, including but not limited to transmitting offensive or harassing messages; offering for sale, use, or purchase any substance the possession or use of which is prohibited by the District's student discipline policy, local, state, or federal law; sending, receiving, viewing, or downloading obscene materials, materials harmful to minors, or materials that depict the sexual exploitation of minors, or materials that encourage others to violate local, state, or federal law; information pertaining to the manufacture of weapons; intruding into the networks or computers of others; and downloading or transmitting confidential, trade secret information, or copyrighted materials;

B. Uses amounting to harassment, sexual harassment, bullying, or cyber-bullying defined as using a computer, computer system, or computer network to convey a message in any format (audio or video, text, graphics photographic, or any combination thereof) that is intended to harm another individual

C. Uses that cause harm to others or damage their property, person or reputation, including but not limited to engaging in defamation (harming another's reputation by lies); employing another's password or some other user identifier that misleads message recipients into believing that someone other than you is communicating; reading another person's communications; sharing another person's pictures, private information, or messages without their permission; or otherwise using his or her access to the network or the internet;

D. Uploading a worm, virus, other harmful form of programming or vandalism; participating in "hacking" activities or any form of unauthorized access to other computers, networks, or other information; or being in possession of hacking software. Users will immediately notify the school's system administrator if they have identified a possible security problem. Users will not go looking for security problems, because this may be construed as an illegal attempt to gain access.

E. Downloading, installing, or copying software or other files without authorization of the Superintendent or the Superintendent's designee, regardless of whether it is copyrighted or de-virused;

F. Uses that are commercial transactions, including commercial or private advertising. Students and other users may not sell or buy anything over the internet. Students and others should not give information to others, including credit card numbers and social security numbers;

G. Uses that jeopardize the security of student access and of the computer network or other networks on the internet; uses that waste District resources including downloading very large files without permission from a teacher, unnecessary printing, and consuming excess file space on shared drives; Users are responsible for making back-up copies as needed;

H. Hacking or gaining unauthorized access to files, resources, or entities; uploading a worm, virus, or other harmful form of programming; failing to take reasonable precautions to protect District equipment from viruses;

I. Attempting to bypass internal or external security systems or controls using District equipment. Students and staff may only access the internet using the District network. The deployment of private wireless access points in classrooms, labs, and offices is prohibited. The District may provide wireless connectivity on a limited basis, depending on need and location;

J. Invading the privacy of individuals, which includes the unauthorized disclosure, dissemination, and use of information of a personal nature about anyone;

K. Using another user's account or password or some other user identifier that misleads message recipients into believing that someone other than you is communicating;

L. Posting material authored or created by another, without his or her consent; Plagiarism of material accessed online. Teachers will instruct students in appropriate research and citation practices;

M. Posting or sending messages anonymously or using a name other than one's own;

N. Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, bullying, or illegal material; and

O. Using the network while access privileges are suspended or revoked;

P. The promotion of election or political campaigns, issues dealing with private or charitable organizations or foundations, ballot issues, or proselytizing in a way that presents such opinions as the view of the District;

Q. Disclosing identifying personal information or arranging to meet persons met on the internet or by electronic communications; sharing one's password with others or allowing them to use one's account;

R. Any other unacceptable uses as outlined in District Policy 3270.

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 students or staff.

D. Recognize that 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.
E. Do not use the network in any way that would disrupt its use by other users.
F. Consider all communications and information accessible via the network 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 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 District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

7. Indemnification: The user agrees to indemnify the District for any losses, costs, or damages (including reasonable attorney fees) incurred by the District, relating to or arising out of any violation of these procedures.

8. 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, Internet Safety Coordinator, or building principal. Do not demonstrate the problem to other users. Keep your account and password confidential, do not let others use your account and password, or leave your account open or unattended. Do not use another individual's account. Attempts to log on to the internet as a system administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to the network. Students may not attempt to defeat or bypass the District's filtering software on any personal or District-owned computer.

9. Vandalism: Vandalism will result in the 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.

10. Telephone Charges: The District assumes no responsibility for any unauthorized charges or fees, including telephone charges, long-distance charges, per-minute surcharges, or equipment or line costs.

11. Copyright Web Publishing Rules: Copyright law and District policy prohibit the republishing of text or graphics found on the internet or on District websites or file servers, without explicit written permission.

    A. For each republication on a website or file server of a graphic or 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 website address of the original source.

B. Students engaged in producing website pages must provide library media specialists with e-mail or hard copy permissions before the website pages are published. Printed evidence of the status of "public domain" documents must be provided.

C. 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.

D. The "fair use" rules governing student reports in classrooms are less stringent and permit limited use of graphics and text.

E. Student work may only be published if there is written permission from both the parent/guardian and the student.

F. Violation of the copyright web publishing rules may result in denial of access to the network.

12. Use of Electronic Mail: Electronic mail (e-mail) is an electronic message sent by or to a user in correspondence with another person having Internet mail access. Students in grades K-5 may be provided e-mail access under direct teacher supervision with a classroom account. Students under the age of 13 may be provided an email account with parent permission. Secondary students may be provided safe, web-based email.

    A. The District's electronic mail system, and its constituent software, hardware, and data files, are owned and controlled by the District. The District provides e-mail to aid students in fulfilling their duties and responsibilities and as an education tool.

    B. Email could be subject to public records requests and disclosures depending upon the subject matter of the contents of the email.

    C. 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 to an electronic mail account is strictly prohibited.

    D. All District email correspondence is backed up and may be utilized for public disclosure requests or disaster recovery. Messages received by the computer network service may be retained on the system until deleted by the recipient. Users are expected to remove old messages in a timely fashion. The system administrators may remove such messages if not attended to regularly by the users

E. Each person should use the same degree of care in drafting an electronic mail message that would be put into a written memorandum or document. Nothing should be transmitted in an e-mail message that would be inappropriate in a letter or memorandum.

F. Electronic messages transmitted via the District's internet gateway carry with them an identification of the user's internet "domain." This domain name is a registered domain name and identifies 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 this District. Users will be held personally responsible for the content of any and all electronic mail messages transmitted to external recipients.

G. Any message received from an unknown sender via the internet should either be immediately deleted or forwarded to the system administrator. 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 file so transmitted.

H. Use of the District's electronic mail system constitutes consent to these regulations.

Violations

Violation of this policy may result in the following disciplinary actions:

1. A student may lose computer privileges/network access. The length of loss will depend on age and severity of the infraction as determined by the system administrator.

2. A student, who has exhibited a pattern of abuse or flagrant violations, continues to engage in serious or persistent misbehavior by violating this policy may lose all computer privileges/network service access for the remainder of the school year or for the duration of school attendance.

3. A student may be removed from the class, suspended, or expelled from school if he or she engages in conduct on the computer network service that constitutes flagrant or persistent violations of this policy or could be considered illegal, as defined by federal and/or state law. Students committing illegal acts may be referred to local law enforcement. Expulsion may be considered for flagrant violations of this policy.

4. Each student is responsible for any damage he or she may cause to this District's computers or to the computer network service. The student must pay all costs incurred in restoring the computer or the network service to its previous working order.

5. If a class requires the use of a computer and/or the computer network service, a student who has lost computer privileges under this policy may be allowed to participate under constant direct teacher supervision unless he or she has been removed from the class.

The Internet Safety Coordinator, in conjunction with the System Administrator and the building principal will make all decisions regarding whether or not a user has violated this policy and any related rules or regulations and may deny, revoke, or suspend access at any time, with his or her decision being final.

If the actions of the individual are also in violation of other District discipline policies, said student shall be subject to additional possible disciplinary action based upon these policies.

The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to any e-mail transmitted on this District's computer network service.

Internet Safety

Because the information and sources of information on the Internet is continually changing, it is impossible for the District to monitor all the content. Users may encounter information that is controversial or potentially harmful.

Each District computer with internet access shall have a filtering device that blocks access 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 District will also monitor the online activities of students, through direct observation and/or technological means, to ensure that students are not accessing such depictions or other material that is inappropriate for minors. This District shall also strive to provide students with the understanding and skills needed to use computer network services in an appropriate manner. The Superintendent or designee shall enforce the use of such filtering devices. Students must use the District's filtered network for all online activities on school grounds or using District equipment.

The term "harmful to minors" is defined by the Communications Act of 1934 (47 USC Section 254 [h][7]), as meaning any picture, image, graphic image file, or other visual depiction that:

1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; or

2. Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; or

3. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

The term "harmful to minors" is defined in Section 18-1514(6), Idaho Code as meaning one or both of the following:

1. The quality of any material or of any performance of any description or representation, in whatever form, of nudity, sexual conduct, sexual excitement, or sado-masochistic abuse, when it:

    A. Appeals to the prurient interest of minors as judged by the average person, applying contemporary community standards; and

    B. Depicts or describes representations or descriptions of nudity, sexual conduct, sexual excitement, or sado-masochistic abuse which are patently offensive to prevailing standards in the adult community with respect to what is suitable material for minors and includes, but is not limited to, patently offensive representations or descriptions of:

        I. Intimate sexual acts, normal or perverted, actual or simulated; or

        II. Masturbation, excretory functions, or lewd exhibits of the genitals or genital area. Nothing herein contained is intended to include or proscribe any matter which, when considered as a whole, and in context in which it is used, possesses serious literary, artistic, political, or scientific value for minors, according to prevailing standards in the adult community, with respect to what is suitable for minors.

2. The quality of any material or of any performance, or of any description or representation, in whatever form, which, as a whole, has the dominant effect of substantially arousing sexual desires in persons under the age of eighteen (18) years.

"Minor" shall refer to an individual who has not attained the age of eighteen (18).

Filtering is only one of a number of techniques used to manage student's access to the internet and encourage acceptable usage. It is not viewed as a foolproof approach to preventing access to material considered inappropriate or harmful to minors. Anything that falls under at least one of the categories below shall be blocked and filtered. This list will be updated/modified as required.

1. Nudity/ pornography: Prevailing U.S. standards for nudity, provocative semi-nudity, sites which contain pornography or links to pornographic sites;
2. Sexuality: Sites which contain material of a mature level, images or descriptions of sexual aids, descriptions of sexual acts or techniques, sites which contain inappropriate personal ads;
3. Violence: Sites which promote violence, images or description of graphically violent acts, graphic autopsy or crime-scene images;
4. Crime: Information on performing criminal acts (e.g., drug or bomb making, computer hacking), illegal file archives (e.g., software piracy);
5. Drug Use: Sites which promote the use of illegal drugs, material advocating the use of illegal drugs (e.g. marijuana, LSD) or abuse of any drug. Exception: material with valid-educational use;

6. Tastelessness: Images or descriptions of excretory acts (e.g., vomiting, urinating), graphic medical images outside of a medical context;
7. Language/Profanity: Passages/words too coarse to be softened by the word filter, profanity within images/sounds/multimedia files, adult humor;
8. Discrimination/Intolerance: Material advocating discrimination (e.g., racial or religious intolerance); sites which promote intolerance, hate, or discrimination;
9. Interactive Mail/Chat: Sites which contain or allow inappropriate email correspondence, sites which contain or allow inappropriate chat areas:
10. Inappropriate Banners: Advertisements containing inappropriate images or words;
11. Gambling: Sites which allow or promote online gambling;
12. Weapons: Sites which promote illegal weapons, sites which promote the use of illegal weapons;
13. Self-Harm: Sites containing content on self harm including cutting, and sites that encourage anorexia, bulimia, etc.; and
14. Judgment Calls: Whether a page is likely to have more questionable material in the future (e.g., sites under construction whose names indicate questionable material)

Filtering should also be used in conjunction with:

1. Educating students to be "Net-smart" , including the dangers of inappropriate content on the Internet; safety and security in the use of electronic mail, chat rooms, and social networking sites; cyberbullying awareness and response; hacking and other unlawful online activities; and the importance of protecting personal information online;
2. Using recognized internet gateways as a searching tool and/or homepage for students, in order to facilitate access to appropriate material;
3. Using "Acceptable Use Agreements";
4. Using behavior management practices for which internet access privileges can be earned or lost; and
5. Appropriate supervision, either in person and/or electronically.

The Internet Safety Coordinator, in conjunction with the System Administrator and the building principal shall monitor student internet access.

Internet filtering software or other technology-based protection systems may be disabled by a supervising teacher or school administrator, as necessary, for purposes of bona fide research or other educational projects being conducted by students age eighteen (18) and older. Disabling of the Internet block or filter system by any other student will result in disciplinary action.

Any staff member, student, parent, or patron may request that the District either block, or disable a block of, a particular website by filing a written request with the Superintendent or his or her designee. The Superintendent will appoint a five (5) member committee, including three (3) staff members and (2) patrons. The committee will meet with the individual who filed the request in a timely manner, allow the individual to make oral or written arguments to support the request, and make a written recommendation to the Superintendent regarding whether the District should block, or disable a block of, a particular website. Upon reviewing the request and the committee's recommendation, the superintendent will render a written decision and notify

the individual who made the request. The Superintendent's decision in the matter will be final.

Review of filtering technology and software shall be done on a periodic basis and is the responsibility of the Internet Safety Coordinator. It shall be the responsibility of the Internet Safety Coordinator to bring to the Superintendent or designee any suggested modification of the filtering system and to address and assure that the filtering system meets the standards of Idaho Code 18-1514 and any other applicable provisions of Chapter 15, Title 18, Idaho Code.

Additionally, Internet access is limited to only those "acceptable uses," as detailed in these procedures. Internet safety is almost assured if users will not engage in "unacceptable uses," as detailed in District policy and procedures, and will otherwise follow District policy and procedures.

Students are prohibited from joining chat rooms, unless it is a teacher-sponsored activity.

Confidentiality of Student Information

Personally identifiable information concerning students may not be disclosed or used in any way on the internet without the permission of a parent or guardian and the student or, if the student is eighteen (18) or over, the permission of the student. Students should be aware that conduct on the District's computer or using the District's server may be subject to public disclosure depending upon the nature of the communication. Users should never give out private or confidential information about themselves or others on the internet, particularly credit card numbers and social security numbers. Staff members may approve exceptions in the case of applications for college or employment. A supervising teacher or administrator may authorize the release of directory information, as defined by law, for internal administrative purposes or approved educational projects and activities.

Student Use of Social Media

Students will be held accountable for the content of the communications that they post on social media websites and are responsible for complying with District policy. Students may not disrupt the learning atmosphere, educational programs, school activities, or the rights of others.

All requirements of this policy apply to use of social media through the District network or equipment or as part of a class assignment.

File Storage

The system administrators reserve the right to set quotas for disk use on the computer system. Users exceeding their quota will be required to delete files to return to compliance. Users may request that their disk quota be increased by submitting a request stating the need for the quota increase. In determining whether to grant the request, the designated administrator will review the space available, and the reason for the request. The decision of the administrator regarding disk use is final, and not appealable. A user who remains in non-compliance of disk space quotas after seven (7) days of notification will have their files removed by a system

administrator.

Student Use of Social Media

Students will be held accountable for the content of the communications that they post on social media locations and are responsible for complying with District policy and procedures for content posted using a District computer, network, or software or when posted during school hours when the student is in attendance at school. Student posts on social media locations outside of school hours and school grounds using a personal computer, network, and software shall be private as long as they do not enter into the educational setting and interfere with the orderly operation of the school. Posts to social network sites using a District computer, network, or software may be subject to public records requests. Students may not disrupt the learning atmosphere, educational programs, school activities, or the rights of others.

All of the requirements and prohibitions in District policy and procedure apply to the use of social media on school grounds, through the District network or using District equipment, or as part of a class assignment.

Blogging Guidelines

Blogs are intended to be a forum for expression, but they are provided as a tool for learning and will be subject to school and/or classroom guidelines. Users are expected to treat "blogspaces" as classroom spaces. Speech that is inappropriate for class is not appropriate in a blog. Users should demonstrate ethical behavior and honor the intellectual property of others by avoiding plagiarism, following copyright law, and citing sources or linking to online references. Users are reminded that inappropriate use may result in disciplinary action as determined by the school administration including suspension of technology privileges, conduct referral, or other disciplinary action as described in the student handbook.

Current User Accounts

The computer network service may occasionally require new registration and information from users to continue the service. Users must notify the designated administrator of any changes/deletions in user information.

A user's access to, and use of, the computer network may be terminated at any time by notifying a system administrator. Accounts which are inactive for more than thirty (30) days may be removed along with that user's files without notice given to the users.

An administrator reserves the right, at their sole discretion, to suspend or terminate users' access to and use of the computer network service upon any violation of this policy. This District's administration, faculty and staff may request the system administrator to deny, revoke, or suspend specific user access.

Warranties/Indemnification

The District makes no warranties of any kind, express or implied, in connection with its provision of access to and use of its computer networks and the internet provided under this policy. The District is not responsible for any information that may be lost, damaged, or unavailable when using the network, or for any information that is retrieved or transmitted via the internet. The District will not be responsible for any unauthorized charges or fees resulting from access to the internet, and any user is fully responsible to the District and shall indemnify and hold the District, its trustees, administrators, teachers, and staff harmless from any and all loss, costs, claims, or damages resulting from such user's access to its computer network and the internet, including but not limited to any fees or charges incurred through purchases of goods or services by the user. The user or, if the user is a minor, the user's parent(s)/legal guardian(s) agrees to cooperate with the District in the event of the school's initiating an investigation of a user's use of his or her access to its computer network and the internet.

Wireless Internet Access

As access to wireless network access equipment becomes more ubiquitous, it is imperative that all implementations of wireless service in the District facilities be provided by the Department of Technology or approved by the Director of Technology. Unauthorized wireless access points not only conflict with the District's physical/wireless network, but may circumvent security measures in place by providing unauthenticated, unsecured network access. Therefore, the deployment of private wireless access points in classrooms, labs, and offices is prohibited.

The District will provide reliable and secure wireless network access based on 802.11 standards. Users of District equipment will be provided wireless connectivity on a limited basis, depending on need and location.

The District provides guest wireless access for visitors to the District.

Procedure History:
Promulgated on: August 11, 2014
Revised:

Coeur d'Alene School District 271

STUDENTS **3265**

Personal Electronic Devices

PERSONAL ELECTRONIC DEVICES (PED)s in the classroom provide opportunities to extend and enrich learning. PEDs allow access to educational digital content and provide students with opportunities for 21st century learning including critical thinking, collaboration and problem solving.

Personal Electronic Devices (PEDs) or portable communication devices are personally owned wireless and/or portable electronic hand-held equipment that include but are not limited to laptops, existing and emerging mobile communication systems and smart technologies with digital audio, photo or video capability (cell phones, smart phones, etc.), portable Internet devices (tablet PCs, ereaders, etc.), hand-held entertainment systems or portable information technology systems that can be used for: word processing, wireless Internet access, image capture/recording, sound recording and information transmitting/receiving/storing, etc. This policy will also apply to new technologies that may be developed for similar purposes.

POLICY REFERENCE
3330 – Student Discipline
3270 – Acceptable Use of Electronic Networks
3295 – Prohibition Against Student Harassment, Intimidation, Bullying and Cyber Bullying
3370 – Search and Seizure

Policy History:
Adopted on: March 3, 2014
Revised on:

Coeur d'Alene School District Student Technology Use Agreement

Coeur d'Alene School District Policies and Procedures 3265 and 3270 guide employees and students in responsible use of information and technology. The International Society for Technology in Education (ISTE) Standards define digital citizenship as an understanding of human, cultural, and societal issues related to technology and the practice of legal and ethical behavior. The following statements explain the expectations for responsible use of technology, access, and digital communication for any school related purpose.

As a digital citizen I will:

- Keep private information private. My password(s) and identity are mine and not to be shared.
- Treat others with respect both online and offline.
- Have appropriate conversations in all my interactions with others.
- Report anyone who tries to use technology tools to hurt or harass me to an appropriate authority (teacher, principal, parent, etc.).
- Strive to be a responsible digital citizen and encourage others to do so as well.
- Credit my sources when I am using other people's information, images or other material.
- Follow Coeur d'Alene School District policies, rules and regulations.
- Exercise care and personal responsibility when using school/district equipment.
- Use my own electronic device(s) at school only with the permission of my parent or guardian and my teacher. I understand my school will have posted guidelines about using my device during lunch and in common areas.
- Use only the BYOD network while using my personal device at school; not my data plan.
- Capture, record or transmit the words and/or images of any staff member or student only with their express permission.

As a digital citizen I understand:

- Internet access is available to further learning goals and objectives.
- Any computer work may be lost and I should be careful to back up important work in more than one location.
- Some things from the Internet I read may not be true.
- Information I post online leaves a "digital footprint" that can have lasting effects.
- Cyber-bullying is a violation of Coeur d'Alene School District policies and I can be subject to disciplinary action if I am bullying others online, even if it's outside of school.
- I may not create, transmit, or communicate any material accessible via the Internet that contains items that are illegal, obscene, harassing, insulting, ostracizing, or intimidating to others.
- The Coeur d'Alene School District does not condone or permit the viewing or use of inappropriate material and uses content filtering software to protect students and staff to the extent possible.
- Content filtering tools are not completely fail-safe. School and district personnel have the authority and responsibility to monitor appropriate use of technology tools. Parents are also encouraged to monitor their child's Internet activity.
- Using a school computer or network is not private; even when generated on a personal device. Teachers and district staff may review my work and activities when I am using a

school log on. Any and all Coeur d'Alene School District log on histories can be inspected.

- My school will have posted guidelines about using my personal device during lunch and in common areas; not following those guidelines may result in my device being confiscated temporarily.
- Accounts may be created for me for school related use on services such as (but not limited to):
    - Clever
    - Brain Honey
    - Google Apps for Education
    - i-Ready
    - Plato
    - Think Through Math
    - Typing Master

  A complete list of services used, along with links to privacy policies and terms can be found on the district website. All services comply with the district student data privacy and security policy 3575. For questions about student accounts, please contact the school office or district technology department.
- Technology use at school is not a right but a privilege. I understand that violating any of these policies may result in this privilege being removed.

I acknowledge that I have read and understand the Coeur d'Alene School District's Student Technology Use Agreement. I agree to abide by all of the applicable rules and regulations. I understand that the District reserves the right to access, review, monitor, audit, log and/or intercept computer/technology use at all times and without prior or subsequent notice. I pledge that I will use technology responsibly and for educational purposes under the direction of school staff. I understand that the use of devices and all technology in the Coeur d'Alene School District is a privilege that can be revoked.

School: _____

Student Printed Name: _____

Student Signature: _____ Date: _____

Parent or Legal Guardian Printed Name: _____

Parent or Legal Guardian Signature: _____ Date: _____

For more information about safe and responsible use of technology and information, please check out Common Sense Media resources for families and students: https://www.commonsensemedia.org/educators/connecting-families/share