Johnstonville Elementary School District
Grade 6-8 Student Acceptable Use Policy for Technology and the Internet

Table of Contents

Page

INTRODUCTION

Johnstonville Elementary School District
Student Acceptable Use Policy for Technology and the Internet

The Johnstonville Elementary School District furnishes computers, network facilities, and access to the Internet to enhance instruction and support an environment conducive to learning. By providing access to the Internet, the District wants to promote excellence in education and prepare you for an increasingly complex world where technology is an essential part of life. The District encourages research, innovation, communication and collaboration.

The District recognizes that access to the Internet also contains material that is unrelated to education and is inappropriate for learning. Because of this potential, the computers, network, Internet, and all other technology owned by the District are to be used only for purposes directly related to school work and student activities.

To maintain the effectiveness of technology purchased for the education of students, all users will be responsible for the proper use and care of assigned equipment. It is our expectation that all users will demonstrate respectful behavior when working with the equipment and software. It only takes one individual to cause serious damage at high costs to the District and taxpayers.

All students agree to abide by all provisions of this policy whether using the technology on site or off site. Your signature and your parent/guardian signature constitute a binding agreement that you have read this policy and agree to abide by its provisions. No person will be allowed to access any computers, network resources, or the Internet without a signed and dated copy of this policy on file.

Students agree to abide by these expectations:

1) Report any problems with your equipment to your teacher, staff member, or the Technology Department.
2) Food and/or beverages are not allowed near or at computer stations.
3) Leave your computer station in the same condition as you found it when you leave.
4) While the District recognizes the value of storage devices in transporting electronic copies of homework, do not use any personal storage devices (CD's, floppies, memory sticks, etc.) in the computers **without prior consent** from the teacher or supervising staff.
5) Unauthorized installation of software on computers is not allowed at any time.
6) Streaming music off the Internet is not allowed.
7) The equipment is to be used by students only during assigned hours and under direct teacher or staff supervision.
8) All users will maintain the security of their login data and report any security problems to their supervising teacher or staff member. **Account usernames and passwords are for that individual person only and shall not be shared with anyone.**
9) **Students are not to share files and/or other electronic information relating to class assignments without the written consent of the teacher. Such acts by a student may be interpreted as "cheating" and may result in disciplinary action up to and including removal from the class with a failing grade.**

10) **Violation of the District Technology Use Policy may result in the user not accessing any computers in the District for an indefinite time. A user who violates the terms of this policy may be subject to disciplinary action and/or may be required to reimburse the District for any costs relating to verifying the integrity of the systems and all repairs necessary to restore those systems affected.**

11) **The following are zero tolerance violations**:

   a. Installing a malicious or viral file to intentionally infect the system.
   b. Downloading or installing any unauthorized software to the computer or systems.
   c. Altering or attempting to alter the computer's operating systems, software, or security systems.
   d. Breaching or attempting to breach the system's security settings or devices.
   e. Any act or attempted act that causes damage to the computer hardware/software and/or peripherals.
   f. Any attempt to breach external sites or resources from Johnstonville systems without prior written approval from all entities involved.
   g. **Viewing or downloading inappropriate content from any source.**
   h. Any attempt made from a remote location to alter or disrupt the District's technology services.

Johnstonville Elementary School District
ELECTRONIC INFORMATION SERVICES

1.0 Purpose

1.1 To provide Johnstonville Elementary School District students with guidelines for proper use of the Internet.

2.0 Scope

2.1 This policy applies to all JESD students using school computers and/or equipment, or private computers whether in the home or on campus to access or in any way utilize the school-provided technology resources. The Internet includes material that is not appropriate for education and inappropriate for learning. The intent of the District is to use technology resources (including the Internet) only for purposes directly related school work and student activities. Anyone who uses the technology illegally or improperly will lose the privilege of using it.

3.0 General

3.1 All users that have a valid Network User ID and Password will have access to the Internet through the District Network. It is the responsibility of the user, before accessing the Internet, to review and understand this document.

3.2 The District Administration and the School Board will periodically review the issues that arise from the use of the Internet and make changes as necessary.

4.0 Policy

4.1 Use of the Internet is a privilege, not a guaranteed right.

4.2 Using District technology in support of illegal activities is prohibited. Any illegal use will be forwarded to the proper authorities.

4.3 Students must observe all copyright laws regarding the use of electronically published work, images, and any other copyrighted works. All material obtained from the Internet must be done so in a manner that respects the publishers' copyrights. If you are unsure of whether you may be violating copyright laws, please ask your teacher or the technology staff.

4.4 The primary use of the Internet is for educational purposes. Use of any school supplied facility or equipment will be monitored, recorded, and reviewed by the District. The District administration reserves the right to access and read Internet messages, review Internet sites visited and monitor users at any time.

4.5 Private student e-mail accounts cannot be accessed from the District network in accordance with CIPA requirements.

4.6 The District's computers, network resources, technology equipment, and the Internet will not be used for personal, commercial, or for-profit endeavors.

4.7 Trademark policies must be adhered to. All resources created using District equipment or software, domain names and trademarks are property of the District and the users have no ownership rights in them.

4.8 You are responsible for protecting your computer and the network systems from viruses and malware (malicious software) that may inadvertently be downloaded from the Internet.

4.9 Always observe proper Netiquette (rules for polite correspondence on the Internet).

- Please be polite! One example of being impolite is using all caps in a sentence, which is considered shouting.
- Do not Flame. An impolite message, a piece of e-mail or a posting which is argumentative or name calling is an example of flaming. Flaming is considered bad manners.
- More information about Netiquette is available on the Internet.

4.10 The Internet is to be considered unsecure and you should refrain from sending sensitive information over the Internet. If you have any doubt as to whether an item should be put on the Internet, contact the technology staff.

4.11 Various tools exist on the Internet to disperse and gather information. Misuse of these tools will not be allowed. It is forbidden to use any of the tools in this account to annoy or harass others. This includes but is not limited to sending or receiving sexually explicit messages, graphics, discriminatory messages, or other inappropriate or illegal activities.

4.11 Any user who connects a storage device (memory stick, CD, floppy disk, etc) to the District's network must be aware that the data and programs on that device are subject to electronic scans. Any file found to contain malware will be modified or deleted from that device. Any programs that may circumvent the security system or cause harm to the computer or network will be modified or deleted. The District shall not be held responsible for any data alteration or deletion that results from such scans.

5.0 Cautions

5.1 The user is responsible for understanding and following these guidelines. Failure to comply with this policy may subject the user to lose technology privileges.

5.2 The Internet is a tool. This policy gives general guidelines to the use of the Internet. The intent of the District is to provide this tool to enhance educational productivity. If the tool is abused, its use could be severely restricted or eliminated.

Johnstonville Elementary School District
Internet Safety Policy

1.0 INTRODUCTION

1.1 It is the policy of the Johnstonville Elementary School District ("The School District") to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act ("CIPA") [Pub. L. No. 106-554 and 47 USC § 254(h)]. It is the goal of this policy not only to prevent and protect, but to educate employees, students, parents and residents of Lassen County in Internet safety.

1.2 The Children's Internet Protection Act, enacted December 21, 2000, requires recipients of federal technology funds to comply with certain Internet filtering and policy requirements. Schools and libraries receiving funds for Internet access and/or internal connection services must also meet the Internet safety policies of the Protecting Children in the 21st Century Act ("PCICA") that addresses the broader issues of electronic messaging, disclosure of personal information of minors, and unlawful online activities.

1.3 This policy is part of the School District's Acceptable Use Policies for Technology and the Internet. All limitations and penalties set forth in the Acceptable Use Policies are deemed to be incorporated into this policy. Terms used in this policy which also appear in the Children's Internet Protection Act have the meanings defined in the Children's Internet Protection Act.

2.0 COMPLIANCE WITH THE REQUIREMENTS OF CIPA:

2.1 **Technology Protection Measures -** A Technology Protection Measure is a specific technology that blocks or filters Internet access. It must protect against access by adults and minors to visual depictions that are obscene, involve child pornography, or are harmful to minors. In addition to the filtering system that is incorporated with the Internet service, the School District subscribes to a content filtering system, on all computers that access the Internet, which is compliant with CIPA and PCICA.

2.2 **Access to Inappropriate Material**

(a) To the extent practical, Technology Protection Measures (or "Internet filters") shall be used to block or filter Internet content or other forms of electronic communications, access to inappropriate information. Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual and textual depictions of material deemed obscene [as defined in section 1460 of title 18, United States Code], child pornography [as defined in section 2256 of title 18, United States Code], or to any material deemed harmful to minors [Defined in section 231 of title 47, United States Code].

(b) Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes.

(c) Any attempt to bypass, defeat, or circumvent the Technology Prevention Measures is punishable as a violation of this policy and of the Acceptable Use Policies.

2.3 Inappropriate Network Usage

(a) To the extent practical, steps shall be taken to promote the safety and security of users of the Johnstonville Elementary School District online computer network when using electronic mail, chat rooms, blogging, instant messaging, online discussions and other forms of direct electronic communications. Without limiting the foregoing, access to such means of communication is strictly limited by the Acceptable Use Policies.

(b) Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes: (1) unauthorized access, including so-called 'hacking,' and other unlawful activities; and (2) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

2.4 Supervision and Monitoring

It shall be the responsibility of all professional employees (pedagogical and administrative staff) of the Johnstonville Elementary School District to supervise and monitor usage of the School District's computers, computer network and access to the Internet in accordance with this policy, the Acceptable Use Policies, and the Children's Internet Protection Act. Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Network Administrator or designated representatives.

2.5 Education

The Johnstonville Elementary School District will advocate and educate employees, students, parents and Lassen County residents on Internet safety and "cyber-bullying." Education will be provided through such means as professional development training and materials to employees, PTA presentations, and community outreach opportunities such as local radio stations and the School District website.

2.6 Cyber-bullying

(a) The Acceptable Use Policies include provisions intended to prohibit and establish penalties for inappropriate and oppressive conduct, including cyber-bullying.

(b) The Johnstonville Elementary School District is a place of tolerance and good manners. Students may not use the network, any District computer facilities, or any electronic device(s) whether used on-campus or off-campus for hate mail, defamatory statements, statements and/or pictures intended to injure or humiliate others by disclosure of personal information (whether true or false), personal attacks on others, and statements expressing animus towards any person or group by reason of race, color, religion, national origin, gender, sexual orientation or disability.

(c) Network users may not use vulgar, derogatory, or obscene language.

(d) Network users may not send or receive vulgar, derogatory, or obscene photographs/graphics regardless of where it originates.

(e) Network users may not post anonymous messages or forge e-mail or other messages.

(f) Furthermore, District computers and network facilities may not be used for any activity, or to transmit any material, that violates United States, California, or local laws. This includes, but is not limited to any threat or act of intimidation or harassment against another person whether from inside or outside the District's network.

CONSENT AND WAIVER

By signing the Consent and Waiver form, I agree to follow the guidelines of the Student Acceptable Use Policy for Technology and the Internet and all District rules and regulations.

Further, I have been advised that the District does not have control of the information on the Internet. Other sites accessible via the Internet may contain material that is illegal, defamatory, inaccurate, or potentially offensive to some people. The District makes no warranties with respect to the District technology services and cannot assume any responsibilities. While the District supports the privacy of technology services, users must assume that this cannot be guaranteed.

The District cannot be held liable for:

- Content of any information or advice received from a source outside the District, or any costs or charges incurred as a result of seeing or accepting such advice
- Any costs, liability, or damage caused by the way a user chooses to use his/her District network access
- Any consequences of service interruptions or changes, even if these disruptions arise from circumstances under the control of the District
- Use of the District network which is inconsistent with the District's primary goals
- Use of the District network for illegal purposes of any kind
- Use of the District network to distribute threatening, obscene, or harassing materials
- Use of the District network to interfere with or disrupt network users, services, or equipment
- Distribution of District information and/or resources, unless permission to do so has been granted by the owners or holders of rights to those resources
- Any consequences arising from monitoring, evaluating, and recording Internet activity information using District technology.

Students agree to abide by all provisions of the District Acceptable Use Policy for Technology and the Internet

We understand that the District may post artwork, writing, photographs, or work for publication on the Internet. In the event anyone requests permission to copy or use the work, those requests will be forwarded to the user or parent/guardian on file. No personal information will appear with such work.

____

Print user name   Date   User ID# (office use)

____

Signature of User

____

Signature of Parent/Guardian   Date

Please sign and return this page.