District Acceptable Use Policy for Technology and the Internet

Table of Contents

Article P*age*

I. Employee Acceptable Use Policy for Technology and the Internet…….…… 2-3
II. Electronic Information Services…….4-5
Purpose……... 4
Scope …… 4
General …….. 4
Policy ……4-5
Cautions ……5
III. Internet Safety Policy……..6-7
Introduction…….6
Compliance with the Requirements of CIPA……..6-7
IV. Internet Publishing Policy …….. 8-10
Goals ……... 8
Acceptable Posting Criteria …… 8
Specific Web Page Guidelines …… 8
Web Page Responsibilities ……. .8-9
Secure Development of Web Pages …… 9
Standards for Web Pages …… 9-10
Suggestions for Successful Page Development ……. .10
V. Consent and Wavier …….. .11

ARTICLE I
JOHNSTONVILLE ELEMENTARY SCHOOL DISTRICT
Employee 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 students 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 the workplace and/or learning. Because of this potential, the computers, network, Internet, and all other technologies owned by the District are to be used only for purposes directly related to work, instruction, and professional development.

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 employees and volunteers agree to abide by all provisions of this policy whether using the technology on site or off site. Your signature constitutes a binding agreement that you have read this policy and agree to abide by its provisions. No employee will be allowed to access any computers, network resources, or the Internet without a signed and dated copy of this policy on file.

All users agree to abide by these expectations:

1) Report any problems with your equipment to the Technology Department via the helpdesk
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) The use of personal storage devices (USB drives, Optical media, etc.) allows employees to work on information and materials on and off site as necessary to perform their job responsibilities. At times when confidential information may be stored on such storage devices, it is the responsibility of the user to protect the contents of this information in compliance with all federal and state laws.
5) Users may not install software, freeware, shareware, or any other application on the District's computers or network. Such an action is not allowed at any time. All requests for software installs will be accompanied by the software licensing information.
6) Listening to music streamed from the Internet without a direct link to instruction is not allowed.
7) When assigned to supervise students who are using the computers, network resources, or the Internet, it is your responsibility to make sure that the Student Acceptable Use Policy for Technology and the Internet is being adhered to by all students.
8) All users will maintain the security of their login data and report any security problems to their supervisor or district administrators. Employee user accounts have greater rights than students; therefore sharing your account information with a student constitutes a violation of federal law. In addition, confidential files and information contained in your account will become visible to anyone with whom you share your account information. **Account usernames and passwords are for that individual person only and shall not be shared with anyone.**
9) **Violation of the District Acceptable Use Policy for Technology and the Internet may result in the user being prohibited from 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.

10) **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 JESD 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.

ARTICLE II
JOHNSTONVILLE ELEMENTARY SCHOOL DISTRICT
ELECTRONIC INFORMATION SERVICES

1.0 Purpose

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

2.0 Scope

2.1 This policy applies to all JESD employees and volunteers 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 the workplace. The intent of the District is to use technology resources (including the Internet) only for purposes directly related to work, instruction, and professional development. 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 Employees must observe all copyright laws regarding the use of electronically published work, computer software, images, and any other copyrighted works. All material obtained from the Internet must be done so in a manner that respects the publishers' copyright.

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 without prior notice.

4.5 Staff Internet e-mail is sent and received via the school e-mail system only in compliance with the Child Internet Protection Act (CIPA). The District provides e-mail accounts for work and school related communications. It is acceptable for staff to receive a reasonable amount of appropriate solicited Internet mail to the school provided e-mail account. If the user wants private e-mail, a personal account with an Internet service provider should be established at the user's expense. Private e-mail accounts cannot be accessed from the District network.

4.6 Employees and volunteers must make use of the District's computers, network resources, technology equipment, and the Internet in an efficient, ethical, and legal manner. These resources will not be used for personal, commercial, or for-profit endeavors.

4.7 Trademark policies must be adhered to. All resources created using District's 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).

- As professionals, 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 inappropriate for the workplace.
- More information about Netiquette is available on the Internet.
- Direct emails to specific persons rather than the entire district user list.
- Brevity is the soul of e-mail.
- Don't use mailing lists to discuss administrative issues. Send these comments to a specific recipient. Double-check to make sure that messages intended for the list go to the list, and messages for administrative issues go to the intended administrator BEFORE you send the message. In general, be very careful using mailing lists and verify recipients before sending.

4.10 The Internet is to be considered unsecure, and you must protect the school's proprietary information from compromise. 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 district administration.

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. You are a representative of the District when on the Internet and, therefore, have the ability to enhance the District's esteem, to damage the reputation of the District, or to place the District in an unfavorable position.

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.

4.12 The District recognizes the value of using personal smart phones to access email provided by the District. Such use is encouraged but the District will not be responsible to reimburse the costs associated with data plans or any other supplemental plans unless specifically required by contract.

5.0 <u>Cautions</u>

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.

ARTICLE III
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 Children in the 21st Century Internet Protection Act (CICPA) 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 CICIPA.

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, and 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], as 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;

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; and

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

(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 Technology Coordinator 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 or any District computer facilities for hate mail, defamatory statements, statements 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 post anonymous messages or forge e-mail or other messages.

(e) 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.

ARTICLE IV
INTERNET PUBLISHING POLICY

1.0 Goals

1.1 To establish the Internet (World Wide Web) as an academic and application tool for student learning, as well as a teaching resource for educators.

1.2 To create an effective communication tool for students, parents, teachers, local community, and the larger educational community.

1.3 To publish exemplary student work as a resource for other students, a celebration of student achievement, and a source of school pride.

2.0 Acceptable Posting Criteria

2.1 Be appropriate (as related to the goals stated above).

2.2 Place acceptable demands on computing and network services.

2.3 Project a positive image of the Johnstonville Elementary School District.

2.4 Protect the safety of students, staff, and their families.

2.5 Comply with all Federal and state rules including Children's Internet Safety Act (CIPA).

3.0 Specific Web Page Guidelines

3.1 All pages posted must be in compliance with copyright laws.

3.2 All web pages must be in compliance with District policies and applicable local, state and federal laws.

3.3 All pages must have a direct relationship to identified student learning targets or other District goals.

3.4 Staff members may only publish student work or photographs (with no names) in electronic form inside a Johnstonville Elementary School District web page. Any exceptions must be submitted in writing to the Technology Coordinator and receive written approval by the Site Administrator or Superintendant.

3.5 All materials displayed on a Web page must be approved by the technology staff or district administration before being published on the Internet. All personally identifiable information must be removed prior to submission.

3.6 The Consent and Waiver form (attached) must be signed by the parent/guardian prior to publishing the student's work (project, essay, art, etc.), identifiable student photograph, or name on the District Web Site. Forms must be filed with the District or other designee.

3.7 Family privacy must be protected. Student work will not reveal home address, home phone, e-mail address, other family details, or personally identifiable information.

3.8 Web pages requiring excessive system resources or network bandwidth or that hamper the efficient operation of the District web site will be shut down and returned for improvement immediately.

3.9 Personal home pages are not to be provided for individual students or staff.

3.10 E-mail links to the supervising teacher/staff member may be provided on student work pages for external feedback.

4.0 Web Page Responsibilities

4.1 The technology staff will provide technical assistance, and insure that District consistency/continuity in its web presence is maintained. The technology staff has the right and responsibility to edit or remove any web pages not conforming to District guidelines or to request that teachers or staff members make appropriate changes.

4.2 Teachers/staff members support the technology staff by creating and providing web page projects, which have been monitored and screened for approval. Teachers/staff members

must approve student work, based on District guidelines, before it can be published "live" on the Internet with links from District or school web pages.

5.0 Secure Development of Web Pages

5.1 Web pages will be developed in a non-public and secure manner, using one of the following three methods only. Web pages (even during development) should be stored in folders, which have names that do not include a student's last name:

6.0 Standards for Web Pages

6.1 Excellence in design and function is encouraged.

6.2 Accuracy is expected. Correct spelling, punctuation, grammar, dates, times, and locations are all vital to facilitate communication and project a professional image for the District. Pages displaying student work should show accuracy and perfection appropriate for that age and skill level.

6.3 Information on pages should be updated in a timely manner. Date of modification or creation should be listed.

6.4 External links must be appropriate for a school audience. The supervising teacher must visit and evaluate each link's first page (and all subsequent links on that first page) for acceptable content. (Inclusion of a link will be viewed by most visitors as "implied endorsement" of that site by the District.)

6.5 External and internal links should be checked regularly (for functionality and appropriate content) and updated or removed as needed.

6.6 Bandwidth is not to be wasted. Download time should be minimized.

6.7 The Main Web Page for a class should:

• Fit on one screen and require no scrolling to see important information.
• Be uncluttered, bright, and welcoming.
• Include the school's postal address, phone number, and an e-mail address of the teacher.
• Contain a link back to the Johnstonville Home Page www.johnstonville.org
• Contain a minimum of large graphics, which should not use more than 50 KB of disk space.
• Avoid "splash screens" and the use of icons as buttons.
• Minimize the use of frames.
• Not contain links to sites outside the District.
• Be written assuming the audience includes:

Students needing to locate external resources quickly;
Students, parents, and local participants interested in internal curricular resources and student products.
Visitors seeking information about the school and its activities.

6.8 Each subsidiary page for a class should be viewed as either a menu page or a content page (document).

- Menu pages should be quick loading, simple, and logically organized, providing visitors with enough information to make a wise choice.
- Twelve to twenty categories are enough for most menu pages.
- Menus should generally avoid excessive scrolling or provide a "hot link" table of contents at the top.
- Content pages should:
    - Include a link back to its menu page or the main page.

- Include a disclaimer whenever individuals may be expressing personal opinions and not those of the school or District.
- Include name of supervising teacher/staff member (where applicable).

6.9 Use easily readable font size and font face, with dark text on a light background or light text on a dark background (and avoid distracting background patterns or textual pages).

7.0 <u>Suggestions for Successful Page Development</u>

7.1 Think before you create! Plan what you want to do, preferably on paper using a storyboard. Map out the hierarchical relationship between all necessary folders and documents. Focus on your intended audience.

7.2 Use relative links and image URLs instead of absolute addresses.

7.3 When naming web files and folders DO NOT USE:

- Spaces in the file name
- Any character other than the alphabet, numbers and the underscore "__"
- Long names (if possible)

CONSENT AND WAIVER

By signing the Consent and Waiver form, I agree to abide by guidelines of the District 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 seeking or accepting such advice
- Any costs, liability, or damage caused by the way a user chooses to use his/her District network access
- Costs associated with the use of any personal mobile device for accessing district email or information
- 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.

Employees agree to abide by the following:

- Computers, network resources, and other District technology shall only be used for educational purposes, work, research, or professional development. Use of these systems for personal, commercial, or for-profit endeavors is not allowed.
- 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

Please sign and return this page.

TECHNOLOGY STAFF USE ONLY
☐AD ☐EM ☐WEB ☐PH