

LAPTOPS FOR LEARNING

ACCEPTABLE USE AND INTERNET SAFETY POLICY FOR THE COMPUTER/INTERNET NETWORK OF THE HOLDREGE PUBLIC SCHOOL DISTRICT

The Holdrege Public School District is pleased to make available to students access to interconnected computer systems within the District and to the Internet, the worldwide network that provides various means of accessing significant educational materials and opportunities. In order for the Holdrege Public School District to be able to continue to make its computer network and Internet access available, all students must take responsibility for appropriate and lawful use of this access. Students must understand that one student's misuse of the network and Internet access may jeopardize the ability of all students to enjoy such access. While the School's teachers and other Staff will make reasonable efforts to supervise student use of network and Internet access, they must have student cooperation in exercising and promoting responsible use of this access.

Listed below are the provisions of your agreement regarding computer network and Internet use. If you have any question about these provisions, you should contact the building principal. If any user violates this Policy, the student's access will be denied, if not already provided, or withdrawn and he or she may be subject to additional disciplinary action.

I. PERSONAL RESPONSIBILITY

By signing the acknowledgement form that accompanies the student handbook, you are agreeing not only to follow the rules in this Policy, but are agreeing to report any misuse of the network to the person designated by the School for such reporting. Misuse means any violations of this Policy or any other use that is not included in the Policy, but has the effect of harming another or his or her property.

II. NETWORK, E-MAIL, INTERNET AND OTHER COMPUTER USE RULES

General Rules:

- a) The network is provided to staff and students to conduct research and communicate with others. Access to network services is given to staff and students who have agreed to act in a responsible manner. Parental permission is required for student use. Access for all staff and students is a privilege and not a right.
- b) Individual users of the district network are responsible for their behavior, actions, problems, and communications involving and over the network. Users will comply with district rules and will honor the agreements they have signed. Beyond clarification of such rules, the district is not responsible for restricting, monitoring, editing, or controlling the information, equipment or communications of individuals utilizing the network or the end product or result of such utilization.
- c) Network storage areas shall be treated like school lockers for students. Network administrators may review files, information, equipment, messages and communications of staff and students to maintain system integrity and insure that users are using the network system responsibly. Users should not expect that files or any information stored or otherwise used or retained on the network, district servers, or in computers, will be private. No reasonable expectation of privacy shall exist in relation to network use.
- d) Users should not expect, and the district does not warrant, any information or products obtained from the network, that files or information stored, obtained or used on the network will be private, and use of the network waives and relinquishes all such privacy rights, interests or claims to confidentiality the user may have under state or federal law.

- e) The district will not be liable for, and does not warrant in any way, purchases made by any user over the network. Users shall not make purchases of goods and/or services via the district's network.

III. ACCEPTABLE USES

Policy and Rules for Acceptable Use of Computers and the Network:

The following policy and rules for acceptable use of computers and the network, including Internet, shall apply to all district administrators, faculty, staff and students. The term "Users", as contained herein, shall apply to all such individuals. The Superintendent, or the Superintendent's designee, is hereby delegated all authority and is the ultimate person in charge of the district network and technology resources or equipment, and the same shall also be under the direct supervision of the site or building administrator where located, sometimes herein called "network administrators."

- a) Users shall not erase, remake, or make unusable anyone else's computer, information, files, programs or disks. In addition to any other disciplinary action or legal action that may occur, any user violating this rule shall be liable for any and all damages to the computer, information, files, programs or disks.
- b) Users shall not let other persons use their name, account, log-on password, or files for any reason (except for authorized staff members).
- c) Users shall not use or try to discover another user's account or password.
- d) Users shall not use the computers or network for non-instructional or non-administrative purposes (e.g., games or activities for personal profit).
- e) Users shall not use the computer for unlawful purposes, such as illegal copying or installation of unauthorized software.
- f) Users shall not copy, change, or transfer any software or documentation provided by teachers, or other students without permission from the network administrators.
- g) Users shall not write, produce, generate, copy, propagate, or attempt to introduce any computer code, software or information designed to self-replicate, damage, or otherwise hinder the performance of the network or any computer's memory, file system, or software. Such software is often called a bug, virus, worm, Trojan horse, or similar name.
- h) Users shall not use the computer to annoy or harass others with language, images, or threats. Users shall not access, accept, create or send any obscene, vulgar, lewd, tasteless, or objectionable messages, information, language, or images.
- i) Users shall not damage the network or equipment, damage information belonging to others, misuse network resources, or allow others to misuse network resources. In addition to any other disciplinary action or legal action that may occur, any user violating this or any other rule shall be liable for any and all damages to the computer, network, information, files, programs or disks.
- j) Users shall not tamper with computers, networks, printers, or other associated equipment except as directed by the teacher or network administrator.

Users shall not take technology equipment (hardware or software) from the school grounds or remove such from computer work areas except as specified through administrative policy. Students and parents will be required to sign agreements to participate in the 1-to-1 initiative.

IV. EDUCATIONAL PURPOSES ONLY

The Holdrege Public School District is providing access to its computer networks and the Internet for only educational purposes. If you have any doubt about whether a contemplated activity is educational, you may consult with the Principal to help you decide if a use is appropriate.

V. NET ETIQUETTE

All users must abide by rules of network etiquette, which include the following:

Etiquette and Rules for Use of Computers and the Network: All users of computers and the network are expected to abide by the generally accepted rules of network etiquette. Informal rules of behavior have evolved for the use of and communication on the network, Internet and other on-line services. Breaches can result in harsh criticism by others. These rules of behavior include (but are not limited to) the following:

- a) Be polite. Do not become abusive in your messages to others.
- b) Use appropriate language. Do not swear, use vulgarities or any other inappropriate language, message, information or images.
- c) Do not reveal your personal account, address or phone numbers, or that of other students or colleagues.
- d) Note that electronic mail (e-mail) is specifically not guaranteed to be private. People who operate the system do have access to mail. Messages relating to or in support of illegal activities may be reported to the authorities. Messages which violate the rules will result in disciplinary action.
- e) All communications and information accessible via the network should be assumed to be private property of others.
- f) Do not place unlawful information on any network system.
- g) Keep paragraphs and messages short and to the point. Focus on one subject per message.
- h) Include your signature at the bottom of e-mail messages. Your signature footer should include your name, position, affiliation, and network or Internet address.
- i) Other rules may be established by the network administrators or teachers from time to time.

VI. INTERNET SAFETY

A. General Warning: Individual Responsibility of Parents and Users

All users and their parents/guardians are advised that access to the electronic network may include the potential for access to materials, inappropriate for school-aged pupils. Every user must take responsibility for his or her use of the computer network and Internet and stay away from these sites. Parents of minors are the best guides to materials to shun. If a student finds that other users are visiting offensive or harmful sites, he or she should report such use to the person designated by the School.

B. Personal Safety

Users are always cautioned to be safe. In using the computer network and Internet, users should not reveal personal information such as a home address or telephone number. Users should not divulge real last names or any other information which might allow a person to locate the user without first obtaining the permission of a supervising teacher. Students should not, under any circumstances, arrange a face-to-face meeting with someone they "meet" on the computer network or Internet without their parent's permission (if students are under 18). Regardless of a student's age, he/she should never agree to meet a person with whom he/she has only communicated on the Internet, and particularly not in a secluded place or in a private setting.

C. "Hacking" and Other Illegal Activities.

It is a violation of this Policy to use the School's computer network or the Internet to gain unauthorized access to other computers or computer systems, or to attempt to gain such

unauthorized access. Any use which violated state or federal law relating to copyright, trade secrets, the distribution of obscene or pornographic materials, or which violates any other applicable law or municipal ordinance, is strictly prohibited.

D. 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, or if the student is 18 or over, the permission of the student himself/herself. Users should never give out private or confidential information about themselves or others on the Internet, particularly home addresses, telephone number, credit card numbers and Social Security numbers. A supervising teacher or administrator may authorize the release of directory information, as defined by state law, for internal administrative purposes or approved educational projects and activities.

E. Active Restriction Measures.

The School, either by itself or in combination with the Educational Service Unit providing Internet access, will utilize filtering software or other technologies to prevent students from accessing visual depictions that are (1) obscene, (2) child pornography, or (3) harmful to minors. The School 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 any other material that is inappropriate for minors. 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 education projects being conducted by students, age 17 and older. 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 taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; 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/or, taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

VII. PRIVACY

Network and Internet access is provided as a tool for the education of every student. The School District reserves the right to 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. All such information files shall be and remain the property of the School District, and no user shall have any expectation of privacy regarding such materials.

VIII. FAILURE TO FOLLOW POLICY

- a) Penalties for Violation of Rules: All of the policies, rules, and procedures for acceptable use of computers and the network are intended to make the computers and the network more reliable for users. They are also intended to minimize the burden of administrating the networks so that more time can be spent on education and enhancing services. Use of the computer and access to telecommunications resources is a privilege and not a right. Violation of the policies, rules, and procedures concerning the use of computers and the network may result in disciplinary action up to, and including, loss of access, suspension and/or expulsion of students from school and loss of access, suspension, termination, non-renewal or cancellation of the contract of administrators, teachers, or other school employees.
- b) Student and Parent Agreements: Students and parents will be required to sign a computer and network use agreement as a condition of the student being permitted to use such equipment.

IX. WARRANTIES/INDEMNIFICATION

The School District makes no warranties of any kind, either express or implied, in connection with its provision of access of and use of its computer networks and the Internet provided under this Policy. It shall not be responsible for any claim, losses, damages or costs (including attorney's fees) of any kind suffered, directly or indirectly, by any user or his or her parent(s) or guardian(s) arising out of the user's use of its computer networks or the Internet under this Policy. By signing the acknowledgment form that accompanies the student handbook, users are taking full responsibility for his or her use, and the user who is 18 or older or, in the case of a user under 18, the parents (s) or guardian (s) are agreeing to indemnify and hold the School, the School District, the Educational Service Unit that provides the Internet access opportunity to the School District and all of their administration, teachers, and staff harmless from any and all loss, costs, claims or damages resulting from the 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) or guardian(s) agree to cooperate with the School in the event of the School's initiating an investigation of a user's activities during his or her access to its computer network and the Internet, whether that use is on a School computer or on another computer outside the School District's network.

X. UPDATES

Users, and if appropriate, the user's parents/guardians, may be asked from time to time to provide new or additional registration and account information or to sign a new Policy, for example, to reflect developments in the law or technology. Such information must be provided by the user (or his/her parent(s) or guardian(s)), or such new Policy must be signed if the user wishes to continue to receive service. If changes occur in some or all of the information a user provides to obtain an account, the user must notify the person designated by the School to receive such information within 72 hours of the change.

Adopted: October 11, 2010