STUDENT PERSONNEL

Internet Safety and Student Acceptable Use of Technologies **5138.1**

It is the policy of Chadron Public School to comply with the Children's Internet Protection Act (CIPA). With respect to the District's computer network, the District shall to the extent practical: (a) prevent user access to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) provide for the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications; (c) prevent unauthorized access, including so-called "hacking," and other unlawful activities online; (d) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (e) implement measures designed to restrict minors' access to materials (visual or non-visual) that are harmful to minors.

1. Definitions. Key terms are as defined in CIPA. "Inappropriate material" for purposes of this policy includes material that is obscene, child pornography, or harmful to minors. The term "harmful to minors" means 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 minors.

2. Access to Inappropriate Material. To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information. Specifically, as required by the CIPA, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. 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.

3. Inappropriate Network Usage. To the extent practical, steps shall be taken to promote the safety and security of users of the District's online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications. Specifically, as required by CIPA, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called 'hacking,' and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

4. Supervision and Monitoring. It shall be the responsibility of all members of the District staff to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and CIPA. Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Superintendent and the Superintendent's designees.

5. Social Networking. Students shall be educated about appropriate online behavior, including interacting with others on social networking websites and in chat rooms, and cyberbullying awareness and response. The plan shall be for all students to be provided education on these subjects. The Superintendent or the Superintendent's designee shall be responsible for identifying educational materials, lessons, and/or programs suitable for the age and maturity level of the students and for ensuring the delivery of such materials, lessons, and/or programs to students.

6. Adoption. This Internet Safety Policy was adopted by the Board at a public meeting, following normal public notice.

Internet Safety and Student Acceptable Use of Technologies **5138.1**

Personal Information & Data

- Students are to have their "Student User Contract" signed by parent(s)/guardian(s) and also the student before any usage of CPS technologies takes place.
- Students are always to use his/her account information to utilize CPS computer(s) and/or network.**
- Students may not share logins/usernames and keys/passwords or any other account information.
- Students may not share, access and/or install any personal information onto CPS technologies or its resources.
- Students may not offer Internet or network access to any other individual via his/her account.
- Students are always to utilize building servers to save their school related files.
- Students may not store, download, and/or transmit any file(s) NOT intended for
- educational purposes. This includes, without limitation: music, video, and graphic file(s).
- Student files can and will be accessed by CPS administrators and its IT department, for recovery and maintenance purposes.
- ALL information stored and/or sent to CPS technologies is considered to be CPS property and should not be considered confidential.
- CPS will accept no responsibility for any use, damage, theft or loss of personal information and/or personal data that is stored within the districts computer(s) and/or server(s).
- CPS will not guarantee the accuracy of the information/data that is stored within the districts computer(s) and/or server(s).

** This may be a building specific rule.

Email Use

- Students may not use CPS technologies and/or its resources to gain access to web-based e-mails such as Hotmail, Yahoo!, Google, etc.
- Students may only access email if school related material is to be transferred and/or transmitted. Such use may be allowed, and WILL be monitored, by a faculty member and/or the IT department.

Computer Usage & Internet Usage

Students may not use CPS technologies and/or its resources for any of the following:

- To create, access, transmit and/or display racist, sexist, defamatory, illegal, indecent, vulgar, pornographic, obscene, threatening, and/or sexually explicit materials or documents which are abusive, harassing, anonymous, and/or contain inappropriate and/or offensive language;
- To transmit, download, access, computer viruses and/or other harmful files and/or programs;
- To harm, alter, and/or destroy any hardware, software and/or data belonging to the school or any other individual;
- To store, download, transmit and/or install software, programs, language code, etc.
- To attach or attempt to attach unauthorized technology devices to CPS technologies or its resources;
- To gain unauthorized access to computer(s), computer network(s), computer file(s). Such as evading or attempting to evade software/network monitoring services (i.e. Internet content filtering software, Firewalls, etc.);
- To hack or attempt anything in relation to computer hacking;
- To violate copyrighted materials in accordance with educational fair use policies;
- To plagiarize other's works;

- For non-educational uses including, without limitation, games, gambling, wagering, junk mail, chain letters, jokes, commercial or private business activities;
- For any non educational streaming of media such as podcasting, internet radio, internet games, and/or anything relating to heavy usage of the district's bandwidth.

Social Networking, Peer to Peer, & Web 2.0

- Students may not use CPS technologies which are not considered at this time to be educational by CPS. (Including, but not limited to: MySpace, Facebook, Xanga, LimeWire, BearShare, Napster, etc.)
- Students may not utilize any type of Web 2.0 program(s)/application(s) including but not limited to eBay, Flickr, iTunes, Youtube, etc. unless authorized by a certified faculty member and/or the IT department.

Risks of MySpace, Facebook and other Social Networking:

Please be advised of the risks associated with using MySpace, Facebook, Xanga, and similar social networking sites.

These sites are public sources of information. The information may be seen by your school administrators, your parents, and law enforcement. It is also accessible to people who you don't even know now, but may later want to impress—such as university admissions and scholarship officials and prospective employers. In fact, many large companies now search the Internet as a means of conducting background checks on job applicants. What you say now on MySpace may affect you years later.

What you say now on MySpace may also affect you right now. Pictures or writings that show that you have violated student conduct rules may result in school discipline. A picture of a student drinking a beer may very well lead to a suspension from activities if the school learns about it. Criminal charges may be filed against you based on information posted on MySpace.

Common sense guidelines to follow when using MySpace and the Internet in general:

- Don't forget that your profile and MySpace forums are public spaces. Don't post anything you wouldn't want the world to know
- (e.g., your phone number, address, IM screens name, or specific whereabouts).
- Avoid posting anything that would make it easy for a stranger to find you, such as where you hang out every day after school.
- People aren't always who they say they are. Be careful about adding strangers to your friends list.
- Harassment, hate speech and inappropriate content should be reported. If you feel someone's behavior is inappropriate report it to MySpace or the authorities.
- Don't post anything that would embarrass you later. Think twice before posting a photo or info you wouldn't want your parents or boss to see!
- Don't mislead people into thinking that you're older or younger. If you lie about your age, MySpace will delete your profile.

Personal Communication Devices, Etc.

- Electronic devices, including but not limited to, cell phones, PDA's, compact disc players, I pods, MP3 players, beepers/pagers, pointers, and/or other mechanical devices that are not required for classroom use or for medical reasons are not allowed in the classrooms or to be used during the school day. If these type devices are utilized inappropriately on CPS campus and/or at CPS activities/functions, then these devices and/or its contents shall be

- confiscated by school personnel. Inappropriate use shall be determined by CPS administrators. (i.e. Inappropriate picture(s) taken at a school sponsored event is considered as a violation of this regulation. The picture(s) taken, through this type device during a school sponsored event, may be considered CPS property).
- CPS is not responsible for the security and safekeeping of students' electronic devices and is not financially responsible for any damage, destruction, or loss of electronic devices.

Administration of Networks

- Maintenance, monitoring, and filtering of CPS technologies and/or its resources shall be done by the CPS IT department.
- Students should notify a building administrator, a faculty member, and/or the IT department of any violations in regards to this AUP by (an)other user(s) or outside parties. This may be done anonymously.
- Other rules/regulations in addition to this policy will be established by the IT department and administration.

Violations of the Acceptable Use Policy

- Violations of the AUP may result in suspension of privileges, permanent loss or termination of privileges, and/or disciplinary measures in according to the district and/or building administrator. All of the rules, regulations, and/or policies within are intended to make CPS technologies and/or its resources more reliable for CPS users.
- Violations of the AUP may also result in legal action if required. This decision shall be determined by the CPS Superintendent and/or CPS administrators.

Adopted: 8-25-08
Amended: 7- 9 -12

Chadron Public Schools
Chadron, Nebraska