China Spring Independent School District
Internet Safety Policy/Acceptable Use Guidelines

The District's Computer Network (hereafter referred to as network) allows users to communicate with other schools, colleges, organizations, and people around the world through the Internet and other electronic information networks. Users will have access to electronic educational resources all over the world.

With this educational opportunity comes responsibility. It is important that you read the District policy (CQ Local) and the Internet Safety Policy/Acceptable Use guidelines and ask questions if you need help in understanding them. Inappropriate network use will result in the loss of the privilege to use this educational tool.

The District will provide training in proper use of the network and will provide all users with access to the Internet Safety Policy/Acceptable Use Guidelines available on the District's web site. All training in the use of the network will emphasize ethical and safe use of this resource. The district will provide for the education of minors about appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms, and cyber bullying awareness and response.

CONSENT REQUIREMENTS

- Copyrighted software or data may not be placed on any device connected to the network without permission from the holder of the copyright. Only the copyright owner, or an individual the owner specifically authorizes, may upload copyrighted material to the network.
- No original work created by any District student or employee will be posted on a Web page under the District's control unless the District has received written consent from the student's parent if the student is a minor.
- No personally identifiable information about a District student will be posted on a Web page under the District's control unless the District has received consent from the student's parent. An exception may be made for "directory information" as allowed by the Family Educational Rights and Privacy Act and District Policy.

FILTERING

- The Superintendent or Designee will maintain appropriate technology for filtering Internet sites containing material considered inappropriate or harmful to minor. All internet access will be filtered for minors and adults on computers with Internet access provided by the school. Upon approval from the superintendent or designee, and administrator, supervisor, or other authorized person may disable the filtering device for bona fide research or other lawful purpose.
- Please note that the Internet is a network of many types of communication and information networks. It is possible that you may run across areas of adult content or some material you (or your parents) might find objectionable. While the District will use filtering technology to restrict access to such material, it is not possible to absolutely prevent such access.
- The categories of material considered inappropriate and to which access will be blocked will include, but not limited to: nudity/pornography; images or descriptions of sexual acts; promotion of violence, illegal use of weapons, drug use, discrimination, or participation in hate groups; instructions for performing criminal acts (e.g. bomb making); on-line gambling.

NETWORK ACCESS

Access to the network will be governed as follows:

- Students in grades K – 3 will be granted access to the network by their teacher, as appropriate.
- Students in grades 4 - 12 will access the network with a unique username and password. All activity will be monitored by CIPA compliant filter and any inappropriate activity will be recorded and reported.
- Students in grades 7-12 will have a My Big Campus account with e-mail.
- Any network user identified as a security risk or as having violated District and/or campus computer use guidelines may be denied access to the network.
- All users will be required to sign a user agreement annually for issuance or renewal of an account.
- Faculty and staff will have e-mail accounts provided by the District. All e-mail will be archived and internet access monitored.

TECHNOLOGY COORDINATOR RESPONSIBILITIES

- The technology coordinator for the network (or campus designee) will:
- Be responsible for disseminating and enforcing applicable District policies and acceptable user guidelines for the network.
- Ensure that employees supervising students who use the network provide training emphasizing the appropriate use of this resource.
- Ensure that all software loaded on computers in the District is not in violation of copyright laws.
- Be authorized to monitor or examine all network activities, including electronic mail transmissions, as deemed appropriate to ensure student safety on-line and proper use of the network.
- Be authorized to establish a retention schedule for messages on any electronic bulletin board and to remove messages posted locally that are deemed to be inappropriate.
- Set limits for data storage within the network as needed.

INDIVIDUAL USER RESPONSIBILITIES

- The following standards will apply to all users of the network.

ON-LINE CONDUCT

- The individual in whose name a network account is issued will be responsible at all times for its proper use.
- The network may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by District policy or guidelines.
- Network users may not disable, or attempt to disable, a filtering device on the network.
- Communications may not be encrypted so as to avoid security review by network administrators.

- Network users may not access another person's network account without the technology coordinators permission, as applicable.
- Students may not distribute personal information about themselves or anyone else and that includes, but is not limited to, personal addresses and telephone numbers.
- Students should never make appointments to meet people whom they meet on-line and should report to a teacher or administrator if they receive any request for such a meeting.
- Network users should avoid actions that are likely to increase the risk of introducing viruses to the network, such as opening e-mail messages from unknown senders and loading data from unprotected computers.
- Network users may not redistribute copyrighted programs or data except with the written permission of the copyright holder or designee. Such permission must be specified in the document or must be obtained directly from the copyright holder or designee in accordance with regulations.
- Network users may not send or post messages that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
- Network users may not purposefully access materials that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
- Network users should be mindful that use of school-related electronic mail addresses might cause some recipients or other readers of that mail to assume they represent the District or school, whether or not that was the user's intention.
- Network users may not waste District resources related to the network.

NETWORK ETIQUETTE

- Network users are expected to observe the following network etiquette:
- Be polite; messages typed in capital letters are the computer equivalent of shouting and are considered rude.
- Use appropriate language; swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language are prohibited.
- Pretending to be someone else when sending/receiving messages is considered inappropriate.
- Be considerate when sending attachments with e-mail by considering whether a file may be too large to be accommodated by the recipient's computer.
- Using the network in such a way that would disrupt the use of the network by other users is prohibited.

PARTICIPATION IN CAMPUS APPROVED CHAT ROOMS, ON-LINE BULLETIN BOARDS, WIKIS, AND OTHER ON-LINE COMMUNICATIONS

- Participation in any chat room, bulletin board, wiki, and other on-line communication will be permitted only for instructional purposes and approved by the campus principal.

CONSEQUENCES FOR INAPPROPRIATE USE

- Suspension of access to the network;
- Revocation of the computer network account; or
- Other disciplinary or legal action, in accordance with the Student Code of Conduct and applicable laws.

VANDALISM PROHIBITED

- Any malicious attempt to harm or destroy District equipment or data or the data of another user of the District's network or of any of the agencies or other networks that are connected to the Internet is prohibited. Deliberate attempts to degrade or disrupt network performance are violations of District policy and administrative regulations and may constitute criminal activity under applicable state and federal laws.
- Vandalism as defined above will result in the cancellation of network use privileges and will require restitution for cost associated with network restoration, as well as other appropriate consequences. {See DH, FN series, FO series, and the Student Code of Conduct}

FORGERY PROHIBITED

- Forgery or attempted forgery of electronic mail messages is prohibited. Attempts to read, delete, copy, or modify the electronic mail of other network users, deliberate interference with the ability of other network users to send/receive electronic mail, or the use of another person's user ID and/or password is prohibited.

INFORMATION CONTENT/THIRD PARTY SUPPLIED INFORMATION

- Network users and parents of students with access to the District's network should be aware of that, despite the District's use of technology protection measures as required by law, use of the network may provide access to other computer Networks in the global electronic network that may contain inaccurate and/or objectionable material.
- A student who gains access to such material is expected to discontinue the access as quickly as possible and to report the incident to the supervising teacher.
- A student knowingly bringing prohibited materials into the school's electronic environment will be subject to suspension of access and/or revocation of privileges on the network and will be subject to disciplinary action in accordance with the Student Code of Conduct.
- An employee knowingly bringing prohibited materials into the school's electronic environment will be subject to disciplinary action in accordance with District policies. {See DH}

DISTRICT WEB SITE

- The District will maintain a District Web site for the purpose of informing employees, students, parents and members of the community of District programs, policies, and practices. The technology coordinator will establish guidelines for the development and format of Web pages controlled by the District.
- No personally identifiable information regarding a student will be published on a Web site controlled by the District without written permission from the student's parent.
- No commercial advertising will be permitted on a Web site controlled by the District.

SCHOOL OR CLASS WEB PAGES

- Teachers will be responsible for compliance with District rules in maintaining their class Web pages.

EXTRACURRICULAR ORGANIZATION WEB PAGES

- Web pages of extracurricular organizations must include the following notice: "This is a student extracurricular organization Web page. Opinions expressed on this page shall not be attributed to the District."

TERMINATION/REVOCATION OF NETWORK USAGE

- Termination of an employee's or student's access for violation of District policies or regulations will be effective on the date the principal or District coordinator receives notice of student withdrawal of revocation of network privileges, or on a future date if so specified in the notice.

DISCLAIMER

- The network is provided on an "as is, as available" basis. The District does not make any warranties, whether express or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the network and any information or software contained therein. The District does not warrant that the functions or services performed by, or that the information or software contained on the network will meet the network user's requirements, or that the network will be uninterrupted or error free, or that defects will be corrected.
- Opinions, advice, services, and all other information expressed by network users, information providers, service providers, or other third-party individuals in the network are those of the providers and not the District.
- The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the network.

ADOPTED

Adopted by the China Spring ISD Board of Trustees at a public meeting on June 18, 2012.

APPROPRIATE USE AGREEMENT

- All users must renew the Agreement for use of the network each academic year.

CHINA SPRING ISD STUDENT AGREEMENT FOR USE OF DISTRICT'S COMPUTER NETWORK

STUDENT NAME_____ SCHOOL YEAR_____
GRADE_____ SCHOOL_____
I understand that my computer use is not private and that the District will monitor my activity on the computer network. I have read the District's Internet Safety Plan/Acceptable Use Agreement and agree to abide by its provisions. I understand that violation of these provisions may result in suspension or revocation of network access.

Student's Signature _____ Date_____

Parent/Guardian Consent:
I have read the District's Internet Safety Plan/Acceptable Use Agreement. In consideration for the privilege of my child using the network, and in consideration for having access to the public networks, I hereby release the District, its operators, and any institutions with which they are affiliated from any and all claims and damages of any nature arising from my child's use of, or inability to use, the network, including, without limitation, the type of damage identified in the District's policy.

☐ I give my permission for my child to participate in the network and certify that the information contained on this form is correct.

☐ I **do not** give my permission for my child to participate in the network

Signature of Parent _____

Date_____ Home phone number_____

CHINA SPRING ISD EMPLOYEE AGREEMENT FOR USE OF DISTRICT'S COMPUTER NETWORK

EMPLOYEE NAME_____ SCHOOL YEAR_____
CAMPUS_____
I understand that my computer use is not private and that the District will monitor my activity on the computer network. I have read the District's Internet Safety Policy/Appropriate Use Agreement and agree to abide by its provisions. I understand that violation of these provisions may result in appropriate disciplinary actions. In consideration for the privilege of using the network, and in consideration for having access to the public networks, I hereby release the District, its operators, and any institutions with which they are affiliated from any and all claims and damages of any nature arising from my use of, or inability to use, the network, including, without limitation, the type of damage identified in the District's policy and administrative regulations.

Signature of Employee_____ Date_____