C.O.O.R. I.S.D.

EMPLOYEE ACCEPTABLE USE
and
INTERNET SAFETY POLICY

It is the policy of C.O.O.R. I.S.D. 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 [Pub. L. No. 106-554 and 47 USC 254(h)].

It is a general policy that all computers used through the C.O.O.R. Network, hereinafter referred to as the Network, are to be used in a responsible, efficient, ethical, and legal manner.

In exchange for the privilege of using the Network, the undersigned agree(s) as follows:

A. The use of the Network is a privilege, **not a right**, which may be revoked by the District at any time and for any reason. Failure to follow the policy and guidelines for the use of Network may result in the loss of privileges, disciplinary action, and/or legal action.

B. 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 Children's Internet Protection Act, 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 for adults or, in the case of minors, minimized only for bona fide research or other lawful purposes. Though the District will make efforts to block/filter inappropriate material, **the District does not guarantee that school officials can control users' access to all such materials, or that users' will not have access to such materials while using District network resources. U**sers may still be exposed to defamatory, inaccurate, or otherwise offensive material. The District specifically denies responsibility for the accuracy or content of information obtained through its services. **The District reserves the right to monitor all internet activity and log internet usage. The District also reserves the right to remove a user account from the network to prevent unauthorized activity.**

C. To the extent practical, steps shall be taken to promote the safety and security of users of the Network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications, including social networking.

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

D. The Children's Online Privacy Protection Act of 1998 [15 U.S.C. 6501] COPPA requires a website that collects personal information for children under the age of 13, parental consent must be obtained. The law permits schools to consent to the collection of personal information on behalf of all of its students. Parental consent constitutes consent for schools to provide personal identifying information for the child consisting of first name, last name, email address and username to selected third party operators (Google, Blackboard, Moodle, etc.)

E. **Staff must maintain the confidentiality of student data in accordance with the Family Education Rights And Privacy Act (FERPA)**

F. Any misuse of the Network access privileges may result in suspension, loss of access privileges and/or other disciplinary action as determined by the District. Misuse includes but is not limited to the following:

1. Use of the District equipment for anything contrary to law, or solicit others to break any law.
2. Illegally copy, install, or distribute any copyrighted software, work, or material. **Copyrighted material must not be placed on any system connected to the District without permission of the copyright holder.**
3. Send, publish, download, access, or retrieve any communication or material, which may be defamatory, abusive, obscene, profane, sexually explicit, threatening, racially or ethnically offensive, harassing, **cyberbullying,** or illegal, or anything that violates or infringes on the rights of any other person.
4. Make any attempt to harm**,** destroy**, or disrupt the operation of the Network, hardware, software, or the data of any other user on this system or any other system. This includes,** but not limited to **uploading,** creating**,** sending**, or knowing transmission of** computer viruses, **spyware,** Trojan horses, or similar **malicious** code.
5. **All information and data stored on District file servers are intended for educational use only. Resources for commercial, for profit, or any other unauthorized purposes (political, advertisements) in any form are prohibited.**
6. Use electronic mail to send unsolicited, bulk, chain, harassing, anonymous, or other messages, which are commonly considered an annoyance to recipients or degrade system performance.
7. Reposting (forwarding) personal communication without the author's prior consent.
8. Using the Network for commercial purpose or financial gain.
9. Use of District Equipment to download, install and play Interactive Internet Games**, online gaming and/or gambling**.

10. Participation in chat rooms unless teacher directed.
11. Attempt to access material or sites that are blocked by the District, or attempt to use the Network while access privileges are suspended.

G. Network resources are to be used exclusively by registered users. **Users are responsible for his/her account and password. The person to whom the account is issued will be responsible for any activity or action performed on the device. Use of any account by someone other than the registered account holder is prohibited.** Users should change their password frequently and should never share their password with another user. Users should never share files without prior approval.

H. Student personal information will not be posted to the District's web site without proper parental/guardian consent.

I. C.O.O.R reserves the right to discipline students for online misbehavior away from school if the actions may harm the school learning environment. This includes cyberbullying. The criteria for cyberbullying are: to physically or emotionally harm someone, there is an unfair match where the victim cannot fairly defend himself/herself and the behavior is repeated (occurs more than once).

J. **Students will be given the opportunity to publish projects, artwork or school work on the World Wide Web in accordance with clear policies and approval process regarding the content that can be loaded to the school's website. Students will continue to retain the copyright on any work published**.

K. Personal information such as complete names, addresses, telephone numbers and identifiable photographs should remain confidential when communicating on the network, **blog, podcast, video, wikis, and social networking site**. Use of free page sites is restricted to the District's system.

L. Student Email is restricted for school use only. Students should not divulge any personal information about himself or herself or any other District student on the Internet. Student email accounts will be restricted to the district addresses only. All other Web based email accounts are prohibited.

M. **Students will never arrange a face-to-face meeting with someone they only know through emails, chats or the internet**

N. The Network user agrees to delete files from his/her home directory on a regular basis in order to avoid unnecessary use of disk space. Users who abuse disk space on the Network will have space restrictions enabled on their Network account and/or lose Network privileges.

O. C.O.O.R. Network administrators will have access to all user accounts and their files. User files are the property of C.O.O.R. **The District reserves the right to monitor and access files, remove files, limit or deny access**

P. The user may not transfer shareware, games or other software from the Internet.

Q. The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages the user

suffers, including but not limited to the loss of data, delays, non-deliveries or service interruptions caused by its negligence or the user's errors or omissions. Use of the Network and any information or data obtained through use of the Network is at your own risk.

R. **Users may be responsible for compensating the school district for any losses, costs, or damages incurred for violations of C.O.O.R's policies/procedures and school rules, including the cost of investigating such violations. The school assumes no responsibility for any unauthorized charges or costs incurred by users while using school district computers, personal devices, school network or any other school technology.**

S. **Students using their own technology in school, such as leaving a mobile phone turned on or using it in class, sending nuisance text messages, or the unauthorized taking of images with a mobile phone camera, still or moving is in direct violation of the school's acceptable use policy.**

T. **The use of personal memory sticks, CD-ROMs or other digital storage media in school requires a teacher's permission.**

U. Users violating any provision of this Acceptable Use Policy face disciplinary action. The District reserves to itself discretion to determine appropriate discipline and will consider the nature and severity of the violation. Possible disciplinary actions include:

1. Suspension of Network access.
2. Require additional training as a precondition to continued use of the Network.
3. Reimbursement for any damages or expense.
4. Discipline action up to and including dismissal.

In addition, the District may refer violations to appropriate law enforcement authorities.

Education, Supervision and Monitoring

It shall be the responsibility of all members of the C.O.O.R. I.S.D. staff to educate, supervise and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act. Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Technology Director or designated representatives. The building Supervisor or designated representatives will provide age appropriate training for students who use the School's Internet facilities. The training provided will be designed to promote the School's commitment to:

a. The standards and acceptable use of Internet services as set forth in the School's Internet Safety Policy;
b. Student safety with regard to:
    i. safety on the Internet;

ii. appropriate behavior while on online, on social networking Web sites, and in chat rooms; and
iii. cyberbullying awareness and response.

c. Compliance with the E-rate requirements of the Children's Internet Protection Act ("CIPA").

Following receipt of this training, the employee will acknowledge that he/she received the training, understood it, and will follow the provisions of the District's acceptable use policies

Helpful Online Safety Sites

http://www.safesurfingkids.com/brochure.htm
http://www.netsmartz.org

EMPLOYEE CONSENT FORM

In consideration of the privilege of using the Network, I hereby release the District, its employees, agents and individual members of the Board of Education from any and all claims or causes of actions arising out of my misuse of the Network and Network equipment. I agree to use the Network responsibly and to abide by the rules and regulations as stated above.

I have reviewed the Acceptable Use and Internet Safety Policy and agree to comply with the policy.

_____ _____

Employee Signature Date

_____

Print Name

I have viewed and passed the assigned School Internet Safety training(s) provided through SET / SEG Safe Schools Training.

_____ _____

Employee Signature Date

_____

Print Name