CiTi

Acceptable-Use Regulation & Agreement

Network Mission

The Network, and through the network, the Internet, offers an abundance of educational material as well as opportunities for collaborations and the exchange of ideas and information. Successful operation requires that all users view the network as a shared resource, and work together to maintain its integrity by behaving in a responsible, conscientious manner.

Privacy Rights

Student and Staff data files and electronic storage areas are considered CITI' property, subject to CITI control and inspection. The system administrator may access all such files and communications to ensure system integrity and that users are complying with the requirements of this regulation and its associated policy. Students and staff should not expect that information stored on the network will be private.

Definition of User

A user is defined as any person that is not a District Official, Administrator of Instructional Technology Personnel that has been assigned a valid network logon by the network administrator. Such logons (for accounts) should be used only by the owner of the account in a legal and ethical fashion.

The Acceptable-Use Regulation

This regulation describes the types of network applications that are contrary to our network mission and which are therefore prohibited. These are guidelines only and are not meant to be an exhaustive list prohibited activities.

Responsibility of Users for Their Account Security

Users are responsible for the use of their individual account and should take all reasonable precautions to prevent others from being able to use their account. Under no conditions should a user provide his or her password to another person. Users will immediately notify the network administrator if they have identified a possible security problem relating to misappropriated passwords.

Illegal or Destructive Activities

Users may not use the network for any purpose that violates the law or threatens the integrity of the network or individual workstations. For example:

Users will not attempt to gain unauthorized access to the network, or go beyond their authorized access. This includes attempting to log on through another person's account or access another person's files, attempting to obtain passwords, or attempting to remove any existing network security functions. Users will not actively search for security problems, because this will be construed as an illegal attempt to gain access.

Users must not intentionally develop or use programs to harass other users to attempt to violate the security or alter software components of any other network, service or system. Examples of such activities include hacking, cracking into, monitoring or using systems without authorization, scanning ports, conducting denial-of-service attacks and distributing viruses or other harmful software.

Users must not attempt to damage hardware, software or data belonging to the school or other users. This includes adding, altering or deleting files or programs on local or network hard drives and removing or damaging equipment such as mice, motherboards, speakers, or printers.

Further examples of unacceptable use include, but are not limited to: fraudulent use of credit card numbers to purchase online merchandise, distributing licensed software or installing software such as games in violation of software license agreements (privacy).

Inappropriate Material

Users will not use the network to access or distribute material that is obscene, pornographic, indecent or hateful, that advocates illegal acts or that advocates violence or discrimination toward other people. This includes but is not restricted to distribution through email, newsgroups or web pages. Exceptions may be made if the purpose of such access is to conduct research and if access is approved by both the teacher and the parent. If a user inadvertently accesses such information, they should immediately disclose the inadvertent access to their teacher of the network administrator.

Respect for Other Users

Restrictions against inappropriate language or images apply to personal email, newsgroup postings and material posted on web pages. Users will not use obscene, profane, vulgar, inflammatory, threatening or disrespectful language. Users will not post false or defamatory information about a person or organization. Users will not post information that, if acted upon, could cause damage to individuals or property.

Users will not harass another person. Harassment is acting in a manner that distresses or annoys another person. This includes, but is not limited to, distribution of unsolicited advertising, chain letters, and email spamming (sending an annoying or unnecessary message to a large number of people). If a user is told by a person to stop sending them messages, the user must stop. Users will not post personal contact information about other people, including address, telephone, home address, work address, etc. Users will not forward a message that was sent to them privately without permission of the person who sent them the message. Users must not send mail that does not accurately identify the sender, the sender's return email address, and the

email address of origin.

Resource Limits

No software shall be downloaded from the Internet or email on the workstation without prior permission from Instructional Technology Personnel. Software installed by any user other than IT personnel is considered a violation of policy. If authorized, users will download the file at a time when the network is not being heavily used immediately remove the file from the network server to their workstation. Users have a right to temporary use of disk storage space and are responsible for keeping their disk usage below the maximum size allocated. Extremely large files, if left on the network for an extended period, may be removed at the discretion of the Director of Technology.

Users will check their email frequently, deleted unwanted messages promptly, and stay within their email quota. Users will subscribe only to discussion group mail lists that advance and are relevant to their education or professional/ career development. Users will unsubscribe to discussion groups before any vacation, break, or other extended absence from school.

Theft of Intellectual Property

Users must respect the legal protection provided by copyright law and license agreements related to content, text, music, computer software and any other protected materials. Users will not plagiarize works that they find on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were original to the user. Users will respect the rights of copyright owners. Copyright infringement occurs when an individual inappropriately reproduces a work that is protected by a copyright. If a work contains language that specifies acceptable use of that work, the user should follow the expressed requirements. If the user is unsure whether or not they can use a work, they should request permission from the copyright owner.

Web Sites/ Personal Safety of Students

Access to the Internet using the CITI' computer equipment is subject to the following restrictions:

Filtering. Filtering software will be used to block minors' access to:

- Visual depictions that are (a) obscene, (b) child pornography, or (c) harmful to minors; and
- Internet sites which, in the Board's determination, contain material that is "inappropriate for minors[1]." (See item B below).

Adult access to visual depictions that are obscene and/or child pornography will also be blocked. However, the Superintendent or his/her designee may disable the software to enable access to blocked sites for bona fide research or other lawful purposes.

[1] The terms "obscene", "child pornography", "harmful to minors" and "matter inappropriate for minors", used throughout the policy, are defined in the Children's Internet Protection Act and the Neighborhood Children's Internet Protection Act (Public Law 106-554) See appendix A.

Matter Inappropriate for Minors. The Board will (from time to time) determine by resolution what Internet material is "inappropriate for minors" in the CITI'. This determination will be based on community standards. (See attachment A).

Safety of Minors When Using Electronic Communications. In using the computer network and Internet, minors are not permitted to reveal personal information such as home address, telephone numbers, their real last names to any other information that might allow someone they are communicating with online to locate them. No minor may arrange a face to face meeting with someone he/she "meets" on the computer network or Internet without his/her parent's permission.

Unauthorized Access and Other Unlawful Activities. It is a violation of this Policy to:

- Use the CITI' computer network or the Internet to gain unauthorized access to other computers or computer systems, or to attempt to gain such unauthorized access;
- Damage, disable or otherwise interfere with the operation of computers, computer systems, software or related equipment through physical action or by electronic means; and/or
- Violate state or federal law relating to copyright, trade secrets, the distibution of obscene or pornographic materials, or any other applicable law or municipal ordinance.

Unauthorized Disclosure and Dissemination or Personal Identification Information Regarding Minors. Personally identifiable information concerning minors may not be disclosed or used in any way on the Internet (e.g., on the [District's or CITI']web page or otherwise) without the permission of a parent or guardian. If a student is 18 or over, the permission may also come from the student himself/ herself.

Regulations and Dissemination. The Superintendent is authorized to develop and implement regulations consistent with this policy. The Superintendent will also be responsible for disseminating the policy and associated regulations to school personnel and students.

Safety and Security. The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communication will be accomplished through disablement of email accounts except under direct teacher supervision and through Internet filtering. Unauthorized access, including so-called "hacking", and other unlawful activity by minors and unauthorized disclosure, use, and dissemination of personal information regarding minors shall be controlled through the use of the district's firewall, Internet filtering and Web Permission form.

Filtering. Internet filtering will be accomplished through use of software and or hardware based technology. Management of this filtering will be conducted by the Instructional Technology Department in cooperation with Administration and Staff. Listed below is a set of categories that will be blocked. Administration or the Director of Technology will only make additions and exceptions to this list after evaluation of the site(s) and approval of the content.

Internet Filtering Categories

Violence/Profanity
Sex Education
Partial Nudity
Gambling/Questionable Illegal
Full Nudity
Alcohol/Tobacco
Sexual Acts
Militant/Extremist
Gross Depictions
Drug Culture
Intolerance

Satanic/Cult

Violation of This Regulation

In the event there is an allegation that a student/ employee has violated the Acceptable-Use Regulation and Agreement, the student/ employee will be provided with a written notice of the alleged violation and an opportunity to present an explanation before an administrator. Disciplinary actions will be tailored to meet specific concerns related to the violation and to assist the student/ employee in gaining the self-discipline necessary to behave appropriately on a computer network. The Director of Technology or the Administration has authority to disable any account where there is a violation of this policy.

The school may at its sole discretion determine whether a use of the network is a violation of this policy. Violations of this policy may result in a demand for immediate removal of offending material, blocked access, suspension or termination of the users account, or other action appropriate to the violation. The school reserves the right to act without notice when necessary, as determined by the administration. The school may involve, and will cooperate with, law enforcement officials if criminal activity is suspected. Violators may also be subject to civil or criminal liability under applicable law.

Agreement

I have read and agree to follow the rules contained in this policy. I understand that if I violate the rules, my account can be terminated, and I may face other disciplinary measures. I hereby release the school, its personnel and any institutions with which it is affiliated from any and all claims and damages of any nature arising from the use of, or inability to use, the system, including but not limited to claims that may arise from the unauthorized use of the system to purchase products or services.

Student

Student Signature
Date
Student Name (Print)
Grade
Home School
Class Name

Legal Guardian

I will instruct my child regarding any restrictions against accessing material that are set forth in the Acceptable-Use Policy. I will emphasize the importance of following the rules for personal safety and give permission to issue an account for my child and certify that the information contained in this form is correct.

Legal Guardian Signature
Date
Legal Guardian Name (print)
Home Address
Phone

Employee/Teacher

Signature
Date
Name (print)
Position
Phone
School or Department

Administrator/Supervisor

Signature
Date
Name (print)
Phone

Appendix A

Generally speaking, “obscenity” is defined as any work that an average person (applying contemporary community standards) would find, taken as a whole, appeals to a prurient interest. The work also must depict or describe, in a patently offensive way, sexual conduct as specifically defined in state law. Moreover, the work taken as a whole has to lack serious literary, artistic, political or scientific value. (See 18 U.S.C. 1460 and the cases interpreting that statute.)

“Child pornography” is defined as:

“… any visual depiction , including a photograph, film, video, picture, or computer or computer generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of visual depiction involves the use of a minor[someone under the age of 18] engaging in sexually explicit conduct; (b) such visual depiction is or appears to be, of a minor engaging is sexually explicit conduct; (c) such visual depiction has been created, adapted, or modified to appear that an identifiable minor in engaging is sexually explicit conduct; or (d) such visual depiction is advertised, promoted, presented, described or distributed in such manner that conveys the impression that the material is or contains a visual depiction of a minor engaging in sexually explicit conduct.” (18 U.S.C. 2256[8]).

The phrase “harmful to minors” is defined as:

“… any picture, image, graphic image, file, or other visual depiction that (a) taken as whole and with respect to minors [defined here as anyone under the age of 17], appeals to a prurient interest in nudity, sex or excretion; (b) depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual contact, actual or simulated normal or perverted sexual acts, or lewd exhibition of the genitals; and (c) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.” (Public Law 106-554,1703[b][2].)

The phrase “matter/ material inappropriate for minors” must be defined by determination by the Board applying local community standards. (Public Law 106-554;1732[1][2].)