**STUDENT INTERNET SAFETY AND NETWORK ACCEPTABLE USE**

The Internet is an international association of computer networks. Government, schools, universities and industry are some of the diverse contributors to the Internet. Access to computer equipment, programs and systems (including hardware and software), the Internet, e-mail and other new technologies (collectively, the “Network”) permit students (“users”) a number of educational and research opportunities they would not have otherwise. While it is the belief of the Great Oaks Institute of Technology and Career Development (the “District”) that such educational benefits outweigh potential disadvantages, the Network may contain content that is inappropriate to the educational setting and that some may consider offensive. The District will be compliant with the requirements of the Children’s Internet Protection Act (CIPA). The District will exercise reasonable guidance to limit student access to such inappropriate materials, but cannot provide assurance that all materials on the Network are appropriate. The district will provide training to secondary students on appropriate online behavior including interactions with other individuals on social networking websites and in chat rooms, with cyber bullying and response.

The ultimate responsibility for monitoring Network usage is that of the student and the student’s parent or guardian.

In exchange for the use of Network resources, either on-site or by remote access, the user understands and agrees to the following.

1. **Privilege:** Access to the Network is a privilege, nota right, and as such it may be revoked by the District at any time and for any reason. The District administrators and/or Network managers may at any time and for any reason perform any or all of the following actions: monitor, inspect, copy, review, and store at any time and without prior notice any and all usage of the Network and any and all materials, files, voicemails, information, software, communications including e-mails, and other content transmitted, received or stored in connection with this usage. The Network and all information, content, e-mails, and files are the property of the District, and users should not have any expectation of privacy regarding those materials.
2. **Acceptable Use:** The Network shall be used primarily for educational purposes. Uses that violate Board policies or interfere with normal Network operations or educational activities, such as those activities described below in “Network Etiquette”, are prohibited. The District may impose restrictions on use of the Network to assure equity of use. As required by law, the District will use filtering programs or other technology protection measures to limit a user’s access to inappropriate materials on the Internet, such as visual depictions that are (1) obscene, (2) child pornography, or (3) harmful to minors. A Network administrator may disable the filtering program or technology protection measure to enable adult users to gain access for bona fide research or other lawful purposes. As required by law, the District will also make reasonable efforts to monitor the user’s online activities, through direct observation and/or technological means, to limit access to such visual depictions or any other materials that are inappropriate to the education setting. As it is impossible to limit access to all materials that may be considered inappropriate, the ultimate responsibility for monitoring Network usage is that of the student and the student’s parent or guardian, and users are required to avoid sites that are inappropriate for the educational setting. The district may also block or filter incoming e-mail.
3. **Access:** Selected Network resources are intended only for use by their registered users. Users shall not have access to the Network until they have signed the Computer Network Information Agreement and completed the Great Oaks Student and Parent Signature Page (if applicable), at which time users shall receive their personal passwords. Access is not transferable and may not be shared. Users shall not share their passwords or otherwise allow anyone to gain unauthorized access to the Network. A user is responsible for any violations of this Agreement committed by someone who, with the user’s express or implied permission, accessed the Network with the user’s password. The President/CEO or Designee shall develop the Network Acceptable Use Student Agreement.
4. **Network Etiquette:** Users shall be held accountable for their use or misuse of the network. All users are responsible for good behavior while using the Network, just as they are in a classroom, in a school hallway, or at any school-sponsored activity. Each user must abide by the rules of Network etiquette, which include but are not limited to the following:
5. Users shall neither obtain copies of nor modify files, other data, or passwords belonging to other users without express authorization from the Campus Dean or designee.
6. Users shall not use the Network to access chat rooms or chat lines. Users shall not use the Network for noncurriculum-related activities (e.g. surfing the Internet, playing games) except for incidental and brief personal communication that does not interfere with the operation of the Network or violate District policies.
7. Users shall not misrepresent themselves or post anonymous messages on the Network. Users shall not forge or falsify e-mail in any way.
8. Users shall not use the Network in any way that would degrade or disrupt the operation of the Network, abuse the software and/or hardware, or excessively consume limited computer, paper, telephone or other resources, such as through spamming, creating or transmitting mass e-mails or chain letters, or other purposes exceeding this policy. Attachments of files to e-mails should not be used.
9. Users are to print only with permission and should be selective when printing. Users are to print one copy and have additional copies made on photocopiers.
10. Users shall not access, create, transmit, copy or download harassing, bullying, threatening, abusive, defamatory, vulgar, discriminatory or sexually explicit messages or materials.
11. Users shall not make rude or hostile reference to race, age, gender, sexual orientation, national origin, disability status, or religious or political beliefs. Abusive or profane language is prohibited.
12. Users shall not reveal any personal information about themselves or other students, including but not limited to photographs, telephone numbers, addresses, passwords, or social security numbers.
13. The confidentiality of any information stored in or created, received or sent over the Network cannot be guaranteed. Users should not have any expectation of privacy regarding such information.
14. Users shall not use the Network for any commercial activities, such as buying advertising or selling goods or services, unless it is for legitimate District business.
15. Except for educational or District business purposes, users shall not create, transmit or download any materials that support or oppose the nomination or election of a candidate for public office or the passage of a levy or bond issue. Additionally, users shall not solicit political contributions through the Network from any person or entity.
16. Users shall not create, transmit, download or copy any materials (1) that are in violation of District Policies or any federal, state or local laws, including but not limited to confidential information, copyrighted materials, material protected by trade secrets, and any materials that would violate the District’s harassment or discrimination policies; or (2) that include the design or detailed information for the purposes of creating an explosive device, materials in furtherance of criminal activities or terrorist acts, threatening materials, or pornographic, sexually explicit or obscene materials.
17. All use of e-mail must be through the District’s e-mail service; the use of other providers of e-mail through the Network is prohibited.
18. Users routinely shall delete outdated or unnecessary e-mails from their mailboxes.
19. All software and hardware must be installed by, or with the prior consent of, the Network administrator. Users may not move, repair, reconfigure, modify, or attach any external devices to Network equipment, including individual computers or systems. Users shall not remove, alter or copy Network software for their own personal use or for the use of others.
20. In utilizing the Network, users shall abide by the standards of academic integrity, including but not limited to plagiarism.
21. When using the District’s Network, the user should remember that he or she is representing the District each time the account is used.
22. **Copyright or License Violations:** The District typically does not own its computer software, rather, it has a license to use the software. All District licensed software shall be reproduced only by authorized systems’ administrators in accordance with the terms of the software licensing agreements. Unauthorized copying, redistribution or republication of copyrighted or licensed material is prohibited.
23. **Websites:** Websites created through the Network and/or linked to the District’s website must relate specifically to educational activities or programs. Websites created using Network or the District’s educational activities or programs, websites created using the Network or the District’s equipment, or websites created as part of the classroom or club assignments or activities are the sole and exclusive property of the District. The District reserves the right to require that material and/or links to other sites found to be objectionable be altered or removed. All web pages under this Policy, other than the official Great Oaks Institute of Technology and Career Development website, must prominently display the following disclaimer:

 This is not an official website of the Great Oak Institute of Technology and Career Development. The Great Oaks Institute of Technology

 and Career Development does not control and cannot guarantee the timeliness or accuracy of the information on this website. Any

 views or opinions expressed herein are solely those of the creators of this website.

1. **Vandalism:** Vandalism is prohibited. Vandalism is any attempt to hack, alter, harm or destroy software, hardware, data of another user, other Network resources, or the use of the Network to harm or destroy anything on the Internet or outside networks. Vandalism includes but is not limited to the uploading, downloading, creating or transmitting of computer viruses, worms, Trojan horses, or other destructive programs or applications.
2. **Security:** If users identify a security problem on the Network, such as evidence of hacking, users shall notify a systems administrator immediately. All users agree to cooperate with the District in the event of an investigation into any allegations of abuse or security breaches of the Network.
3. **Service Disclaimer:** The District makes no warranties of any kind, whether expressed or implied, for the Network services it provides. The District will not be responsible for any damages a user may suffer arising out of the user’s use of, or inability to use, the Network, including but not limited to the loss of data resulting from delays, non-deliveries, misdeliveries, service interruptions, or user errors or omissions. Each user is responsible for backing up his or her files. The District is not responsible for the accuracy of information obtained through electronic information resources; hence, this information should be used at the user’s own risk. The District is not responsible or liable for the security of any personal e-mail, Internet or other transactions of users. The District also is not liable for any transactions, costs, damages or fees incurred by a user through purchases of goods or services or other transactions through the Network or for any illegal actions, including copyright violations, that a user performs through the Network.
4. **Violations of this Policy:** Violations of this Policy may result in disciplinary action, including but not limited to restriction or termination of access to the Network, and/or other discipline in accordance with Policy and Rules and Regulations 5131, Student Code of Conduct. Violations also may be referred to the appropriate legal authorities and/or other legal action may be pursued. Personal information may be released to appropriate entities as the District deems necessary, in its sole discretion, to avoid immediate danger of physical harm to persons or property, or to report possible crimes to the legal authorities.
5. **Changes:** Due to the rapid change in technology, a user’s access and/or this Policy are subject to change at any time.

CROSS REFERENCE: Children’s Internet Protection Act (CIPA)