Network Acceptable Use Policy

Grove City Christian School recognizes that new technologies, such as use of computers, devices attached to a network, electronic communication and the Internet, open opportunities to new information and types of communication. The use of these resources and tools is a privilege. These technologies can have a direct impact in instruction and student learning. The School supports the access to, and use of, appropriate resources by staff and students ("users") for educational purposes and other legitimate school business based on the user's legitimate needs. Due to the nature of technology and the rapid rate of change that encompasses these technologies, a user's access and/or this policy are subject to change at any time.

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

A. Privilege

Access to the Network (school owned devices, email and the Internet including the use of personally owned devices) is a privilege, not a right. Accordingly, access requires responsible and lawful use that honors God. As a privilege, the use of the Network may be revoked by the school administration at any time and for any reason. School administrators and/or Network managers may perform the following actions for any legitimate reasons including but not limited to, for the purpose of maintaining system integrity and insuring that users are using the Network consistent with this policy and with the Children's Internet Protection Act: 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, information, software, communications, and other content transmitted, received, or stored in connection with this usage. The Network and all information, content, and files are the property of the School and users should not have any expectation of privacy regarding these materials.

B. Acceptable Use

The Network shall be used primarily for educational purposes and legitimate school business purposes. The School may monitor the Network and user's online activities. The School will employ filtering programs designed to limit a user's access to inappropriate materials, such as written or visual depictions that are (1) obscene, (2) child pornography, or (3) harmful to minors. As it is impossible to limit access to all materials that may be considered to be inappropriate, users are responsible for their use of the Network and are required to avoid uses of the Network that are inappropriate for the educational setting and/or dishonoring to God.

The Education Committee expects that the school administration will provide guidance and instruction to the students in the appropriate use of these technologies including the Internet. Such training shall include, but not be limited to, education concerning appropriate on-line behavior, including interacting with other individuals on social networking Web sites and in chat rooms and cyber-bullying awareness including appropriate responses to such activity.

C. Access

Selected Network resources are intended only for the use of Grove City Christian School students, staff and other registered users. Access is not transferable and may not be shared.

Any and all use of electronic devices (personally owned or school owned) is subject to the direction of faculty and staff.

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, accesses the Network with the user's password.

Access to the Network resources from outside the school Network system is only permitted via secure VPN (Virtual Private Network) connection by authorized staff. Access to school web-enabled systems is permitted via a Web browser using a secure connection (e.g. https).

Access to the Network resources using personally owned equipment such as computers, mobile devices, Web-enabled devices, and cell phones is permitted only on the wireless network and is subject to the same type and level of activity and material monitoring.

D. Network Etiquette

Use of the Network has great potential to enhance the productivity of the users. The Network, however, could be abused. Users shall be 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, hallway or at any school-sponsored activity. Each user must abide by generally accepted rules of Network etiquette, which include but are not limited to:

1. Users shall communicate only in ways that are God-honoring: kind, responsible, respectful and lawful.
2. Users shall not attempt to circumvent Network security or Internet filter security.
3. Users shall not obtain copies of, or modify files, other data, or passwords belonging to other users without express authorization.
4. Users shall not misrepresent themselves on the Network.
5. Users shall not use the Network in any way that would disrupt the operation of the Network. They shall not intentionally abuse software and/or hardware; use the Network for spamming, changing the device configuration, create or transmit mass emails or chain letters, or extensively use the Network for non-curricular communications or other purposes exceeding this policy.
6. Users shall not create or transmit harassing, threatening, abusive, defamatory or vulgar messages or materials.
7. Users shall not photograph or videotape other individuals and subsequently post these images or videos to the Internet except for educational purposes and legitimate school business purposes.
8. Except for educational or professional purposes, users shall not reveal any personal information beyond directory information about themselves, school personnel, volunteers or students, including but not limited to passwords or social security numbers. Requests for information should be scrutinized by standards of public disclosure, pertinent open records laws and other policies of the school and/or the church.

9. Users shall not presume the confidentiality of any information stored in or created, received or sent over the Network.
10. Users shall not use the Network for any commercial activities, such as buying, advertising, or selling goods or services, unless it is for legitimate school business.
11. Users shall not create, transmit or download any materials that support or oppose the nomination or elections of a candidate for public office unless for legitimate classroom educational purposes. Additionally, users shall not solicit political contributions through the Network from any person or entity.
12. Users shall not create, transmit, download or copy any materials (a) that are in violation of school 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 school harassment or discrimination policies; or (b) that include the design or detailed information for the purposes of creating an explosive device, materials in the furtherance of criminal activities or terrorist acts, threatening materials, or pornographic, sexually explicit or obscene materials.
13. Users shall cite proper credit for any material (text and images) gathered using information technology, using all resources in a manner, which promotes academic integrity, and only to the degree allowed by Federal copyright laws.
14. Users shall respect the registration policies of age-restricted online services.
15. Users shall speak with a trusted adult should you receive an inappropriate message or one that makes you feel uncomfortable.
16. Users shall comply with requests to silence, turn off, or put away electronic devices promptly.
17. Users shall routinely delete unnecessary emails from their GCCS account.

E. Vandalism

Vandalism is prohibited. Vandalism is any malicious 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 intentional uploading, downloading, creating or transmitting of computer viruses, worms, Trojan horses, keystroke loggers, or other disruptive programs or applications.

F. Security

If users identify a security problem on the Network, such as evidence of hacking, users must notify a principal who will then notify the IT systems administrator immediately. All users agree to cooperate with the School in the event of an investigation into any allegations of abuse or security breaches of the Network.

The School and Grove City Church of the Nazarene are not responsible for damages, loss, theft or any costs incurred to personal technologies or electronic communication devices.

G. Service Disclaimer

The School makes no warranties of any kind, whether expressed, or implied, for the Network services it provides. The school 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. The School is not responsible for the accuracy of information obtained through electronic information resources (i.e. electronic library); hence, this information should be used at the user's own risk.

H. 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. Violations also may be referred to the appropriate legal authorities and/or other legal action may be pursued.

I. Signed Authorization Form

All employees must complete a Network Acceptable Use Agreement form annually. The signed forms will be kept in the Human Resource office.

Students in grades 5-12 must complete a Network Acceptable Use Agreement form annually. The signed forms will be kept in the appropriate principal's office.

H.R. 4577, P.L 106-554, Children's Internet Protection Act of 2000
47 U.S.C 254(h), (1) Communications Act of 1934, as amended
20 U.S.C. 6801 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended
18 U.S.C. 2256
18 U.S.C. 1460
18 U.S.C. 2246
76 F.R. 56295, 56303